

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA (SWZ)  
na „Wdrożenie i świadczenie usługi SOC (Security Operation Center)”

oznaczenie niniejszego postępowania: DOA.201.2.2026

TRYB UDZIELENIA ZAMÓWIENIA: tryb podstawowy z możliwością prowadzenia negocjacji (art. 275 pkt 2 ustawy Prawo zamówień publicznych)

Zatwierdził:

Warszawa, dnia 23.03.2026 r.

.....

## I. Spis treści

II.	Nazwa oraz adres Zamawiającego .....	3
III.	Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia .....	3
IV.	Tryb udzielenia zamówienia .....	3
V.	Informacja, czy Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji .....	4
VI.	Opis przedmiotu zamówienia .....	4
VII.	Przedmiotowe środki dowodowe .....	6
VIII.	Termin wykonania zamówienia .....	7
IX.	Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy .....	7
X.	Informacje o środkach komunikacji elektronicznej, przy użyciu których Zamawiający będzie komunikował się z Wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej .....	7
XI.	Wskazanie osób uprawnionych do komunikowania się z Wykonawcami .....	10
XII.	Termin związania ofertą .....	10
XIII.	Opis sposobu przygotowania oferty .....	10
XIV.	Sposób oraz termin składania ofert .....	14
XV.	Termin otwarcia ofert .....	14
XVI.	Podstawy wykluczenia .....	14
XVII.	Warunki udziału w postępowaniu .....	15
XVIII.	Wykaz podmiotowych środków dowodowych .....	17
XIX.	Sposób obliczenia ceny .....	18
XX.	Opis kryteriów oceny ofert, wraz z podaniem wag tych kryteriów i sposobu oceny ofert .....	19
XXI.	Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego .....	20
XXII.	Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy .....	20
XXIII.	Obowiązek informacyjny wynikający z art. 13 RODO .....	21
XXIV.	Spis załączników do SWZ .....	23

## II. Nazwa oraz adres Zamawiającego

Urząd Ochrony Danych Osobowych  
ul. Stanisława Moniuszki 1A, 00-014 Warszawa  
tel. 22 531 03 00

Adres poczty elektronicznej: [przetargi@uodo.gov.pl](mailto:przetargi@uodo.gov.pl)

## III. Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia

Adres strony internetowej prowadzonego postępowania: link prowadzący bezpośrednio (po zalogowaniu się na konto użytkownika) do rozbudowanego widoku postępowania na Platformie e - Zamówienia, umożliwiającego wykorzystanie pełnej funkcjonalności Platformy, w tym do m. in. złożenia oferty oraz komunikacji z Zamawiającym:

<https://ezamowienia.gov.pl/mp-client/tenders/ocds-148610-c063628b-9e6c-49c1-9288-6f4cdeff5895>

Identyfikator (ID) postępowania na Platformie e – Zamówienia:

ocds-148610-c063628b-9e6c-49c1-9288-6f4cdeff5895

Na tej stronie udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z prowadzonym postępowaniem.

## IV. Tryb udzielenia zamówienia

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, na podstawie art. 275 pkt 2 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320 ze zm.), zwanej dalej także „Pzp”.
2. Zamawiający zastrzega, że może unieważnić postępowanie o udzielenie zamówienia, jeżeli środki publiczne, które zamierza przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostaną mu przyznane (art. 310 Pzp).
3. Zamawiający może unieważnić postępowanie również stosownie do art. 256 Pzp przed upływem terminu składania ofert, jeżeli wystąpią okoliczności powodujące, że dalsze prowadzenie postępowania jest nieuzasadnione.
4. Zamawiający zastrzega, że może unieważnić postępowanie o udzielenie zamówienia, gdy cena najkorzystniejszej oferty przewyższa kwotę, którą Zamawiający może przeznaczyć na sfinansowanie zamówienia chyba, że Zamawiający może zwiększyć tę kwotę do ceny lub kosztu najkorzystniejszej oferty.

## V. Informacja, czy Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji

1. Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
2. Zamawiający może wybrać najkorzystniejszą ze złożonych ofert bez przeprowadzania negocjacji. Zamawiający zastrzega sobie możliwość negocjowania z nie więcej, niż trzema Wykonawcami, którzy złożą w odpowiedzi na ogłoszenie najkorzystniejsze oferty.
3. Negocjacje mogą odbywać się osobiście lub przy pomocy elektronicznych środków komunikacji na odległość.
4. Negocjacje nie mogą dotyczyć SWZ. Negocjacje mogą dotyczyć wyłącznie tych elementów treści ofert, które podlegają ocenie w ramach kryteriów oceny ofert. Zakres ewentualnych negocjacji zostanie przez Zamawiającego określony w Zaproszeniu do negocjacji.
5. Po zakończeniu negocjacji Zamawiający wezwie Wykonawców, z którymi prowadził negocjacje do złożenia ofert dodatkowych. Sposób składania ofert dodatkowych, termin na ich złożenie, nie krótszy niż 5 dni oraz termin ich otwarcia zostaną określone w Zaproszeniu do złożenia ofert dodatkowych.
6. Wykonawca może złożyć ofertę dodatkową, która zawiera nowe propozycje w zakresie treści oferty podlegających ocenie w ramach kryteriów oceny ofert wskazanych przez Zamawiającego w Zaproszeniu do negocjacji. Oferta dodatkowa nie może być mniej korzystna w żadnym z kryteriów oceny ofert niż oferta złożona w odpowiedzi na ogłoszenie.

## VI. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest:
  - 1) wdrożenia i uruchomienie usługi SOC (Security Operation Center) u Zamawiającego;
  - 2) świadczenie usługi SOC jako usługi (Security Operations Center as a Service) z wykorzystaniem systemu dostarczonego przez Wykonawcę.

Celem niniejszego zamówienia jest wdrożenie, a następnie utrzymanie stałego monitoringu bezpieczeństwa infrastruktury IT Zamawiającego.

2. Realizacja przedmiotu umowy jest współfinansowana z funduszy Unii Europejskiej w ramach projektu grantowego nr KPOD.05.10-CR.01-001/24/0050/KPOD.05.10-CR.01-001/25/2025 pt. „Cyberbezpieczny rząd” finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd. Projekt grantowy w celu poprawy cyberbezpieczeństwa dla grupy podmiotów krajowego systemu cyberbezpieczeństwa.

3. Nazwa i kody zamówienia według Wspólnego Słownika Zamówień (CPV):
- 72000000-5 – Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia;
  - 72240000-9 – Usługi analizy systemu i programowania;
  - 72222300-0 – Usługi w zakresie technologii informacji;
  - 72511000-0 – Usługi zarządzania oprogramowaniem sieciowym;
  - 72222000-7 – Usługi w zakresie systemów informacji lub strategicznej analizy technologicznej;
  - 72500000-0 – Usługi komputerowe (w tym przetwarzanie danych);
  - 72300000-8 – Usługi w zakresie danych;
  - 72315000-6 – Usługi zarządzania siecią danych oraz usługi wspierające;
  - 72316000-3 – Usługi analizy danych;
  - 72317000-0 – Usługi przechowywania danych;
  - 72611000-6 – Usługi w zakresie wsparcia technicznego.
4. Jeżeli w dokumentach zamówienia zostały wskazane normy, certyfikaty, specyfikacje techniczne lub systemy odniesienia Zamawiający, zgodnie z art. 99 ust. 5 Pzp, dopuszcza rozwiązania równoważne. Wykonawca, który powołuje się na rozwiązania równoważne, zobowiązany jest wykazać, że oferowane przez niego rozwiązania spełniają wymagania określone przez Zamawiającego. Dowodem na równoważność może być np. świadectwo jakości, certyfikat potwierdzający zgodność z inną, co najmniej równoważną normą. Dowody na potwierdzenie ww. Wykonawca składa wraz z ofertą.
5. Zamawiający nie przewiduje udzielenia zamówienia w częściach.
6. Usługa SOC stanowi zintegrowany i ciągły proces obejmujący m.in. monitorowanie bezpieczeństwa systemów informatycznych, analizę zdarzeń bezpieczeństwa, obsługę incydentów, korelację logów, utrzymanie platform SIEM oraz reagowanie na zagrożenia w trybie 24/7/365. Poszczególne elementy tej usługi są ze sobą ściśle powiązane technologicznie i organizacyjnie, a ich realizacja przez jednego Wykonawcę zapewnia spójność procesów bezpieczeństwa oraz jednolitą odpowiedzialność za obsługę incydentów. Ponadto, koordynacja działań wielu Wykonawców realizujących poszczególne elementy usług SOC generowałaby dodatkowe koszty organizacyjne oraz ryzyko sporów kompetencyjnych w zakresie odpowiedzialności za obsługę incydentów bezpieczeństwa. Podział zamówienia na części nie jest uzasadniony ze względów technicznych, organizacyjnych oraz bezpieczeństwa systemów informatycznych, a realizacja zamówienia przez jednego Wykonawcę zapewni jego prawidłowe i efektywne wykonanie.
7. Zamawiający dopuszcza powierzenie podwykonawcom wykonanie części zamówienia.

8. Zamawiający wymaga, aby Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom wraz z podaniem firm podwykonawców, o ile są mu one wiadome na etapie składania ofert.
9. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia. Wykonawca będzie odpowiedzialny za działania, uchybienia i zaniedbania podwykonawców i ich pracowników w takim samym stopniu jakby to były działania, uchybienia i zaniedbania jego własnych pracowników.
10. Zamawiający nie dopuszcza możliwości udziału w postępowaniu Wykonawców, podwykonawców oraz podmiotów udostępniających zasoby z państw trzecich, które nie są objęte porozumieniem GPA i nie są stroną innych umów z Unią Europejską. Zamawiający nie dopuszcza udziału:
  - 1) Wykonawcy prowadzącego działalność oraz mającego siedzibę w państwie trzecim nieobjętym umowami,
  - 2) Wykonawcy wspólnie ubiegającego się o zamówienie z Wykonawcami z państw trzecich nieobjętych umowami,
  - 3) Wykonawcy, który ubiega się o zamówienie, polegając na zasobach podmiotów pochodzących z państw trzecich nieobjętych umowami,
  - 4) Wykonawcy, który ubiega się o zamówienie, powierzając wykonanie części zamówienia podwykonawcom lub dalszym podwykonawcom pochodzącym z państw trzecich nieobjętych umowami.
11. Wykonawca musi realizować wszystkie opisane w wymaganiach zadania na rzecz Zamawiającego korzystając z zasobów usytuowanych na terenie Unii Europejskiej.
12. Wykonawca musi posiadać i utrzymywać przez cały okres umowy:
  - 1) certyfikat ISO27001 oraz ISO22301, co najmniej w zakresie obsługi zgłoszeń i reakcji na incydenty bezpieczeństwa;
  - 2) środowisko SOC spełniające wymagania KRI, KSC oraz RODO;
  - 3) możliwość świadczenia usług 24/7/365.
13. Pozostałe warunki i wymagania przedmiotu zamówienia zostały określone w załączniku nr 1 do SWZ – Opis przedmiotu zamówienia oraz w załączniku nr 2 do SWZ – Projektowane postanowienia umowy.

## VII. Przedmiotowe środki dowodowe

1. Zamawiający wymaga złożenia wraz z ofertą przedmiotowego środka dowodowego w postaci wypełnionej ankiety bezpieczeństwa – stanowiącej załącznik nr 3 do SWZ.
2. Jeżeli Wykonawca nie złoży powyższego przedmiotowego środka dowodowego lub złożony środek dowodowy będzie niekompletny, Zamawiający wezwie do jego złożenia lub uzupełnienia w wyznaczonym terminie.



3. Zamawiający nie będzie wzywał Wykonawców do złożenia lub uzupełnienia przedmiotowego środka dowodowego, jeżeli pomimo złożenia oferta Wykonawcy podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.

## VIII. Termin wykonania zamówienia

1. Wykonawca zobowiązany jest zrealizować przedmiot zamówienia w terminie:
  - 1) etap wdrożenia i uruchomienia – do 30 dni od dnia zawarcia umowy;
  - 2) świadczenie usługi – 12 miesięcy od dnia podpisania protokołu odbioru bez uwag oraz zastrzeżeń, potwierdzającego zakończenie wdrożenia usługi SOC.
2. Maksymalny całkowity czas realizacji – 13 miesięcy.

## IX. Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy

Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy, określone zostały w załączniku nr 2 do SWZ.

## X. Informacje o środkach komunikacji elektronicznej, przy użyciu których Zamawiający będzie komunikował się z Wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej

1. W postępowaniu komunikacja między Zamawiającym a Wykonawcami, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń, odbywa się przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513), tj. za pośrednictwem Platformy e-Zamówienia (zwana dalej Platformą), która jest dostępna pod adresem <https://ezamowienia.gov.pl>.
2. Korzystanie z Platformy e-Zamówienia jest bezpłatne.
3. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego musi posiadać konto podmiotu „Wykonawca” na Platformie e-Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej <https://ezamowienia.gov.pl> oraz informacje zamieszczone w zakładce „Centrum pomocy”.
4. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie ani logowania.
5. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe odwzorowania) musi być zgodne z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie

- sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub w konkursie.
6. Dokumenty elektroniczne, o których mowa w § 2 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub w konkursie, zwanym dalej również „rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych”, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwanego dalej także „rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności”, z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki.
7. Informacje, oświadczenia lub dokumenty, inne niż wymienione w § 2 ust. 1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych, przekazywane w postępowaniu sporządza się w postaci elektronicznej:
- 1) w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (i przekazuje się jako załącznik), lub
  - 2) jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej (np. w treści wiadomości e-mail lub w treści „Formularza do komunikacji”).
8. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2026 r. poz. 85) Wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”.
9. Komunikacja w postępowaniu, z wyłączeniem składania ofert, odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce „Formularze” („Formularze do komunikacji”). Za pośrednictwem „Formularzy do komunikacji” odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk „dodaj załącznik”).



10. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o udzielenie wyjaśnień dotyczących treści SWZ, Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SWZ wpłynie po upływie terminu, o którym mowa powyżej, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
11. W przypadku załączników, które są zgodnie z Pzp lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być opatrzone, zgodnie z wyborem Wykonawcy/Wykonawców wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby, podpisem typu zewnętrznego lub wewnętrznego. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
12. Możliwość korzystania w postępowaniu z „Formularzy do komunikacji” w pełnym zakresie wymaga posiadania konta „Wykonawcy” na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Do korzystania z „Formularzy do komunikacji” służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie.
13. Wszystkie wysłane i odebrane w postępowaniu przez Wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce „Komunikacja”.
14. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji” wynosi 25 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
15. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia.
16. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego poprzez formularz udostępniony na stronie internetowej <https://ezamowienia.gov.pl> w zakładce „Zgłoś problem”.
17. W szczególnie uzasadnionych przypadkach uniemożliwiających komunikację Wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres e-mail: [przetargi@uodo.gov.pl](mailto:przetargi@uodo.gov.pl) (nie dotyczy składania ofert w postępowaniu).

18. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.

## XI. Wskazanie osób uprawnionych do komunikowania się z Wykonawcami

1. Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami: Justyna Różycka, Monika Wilczyńska, e-mail: [przetargi@uodo.gov.pl](mailto:przetargi@uodo.gov.pl)
2. Komunikacja za pośrednictwem poczty elektronicznej jest dopuszczalna w odniesieniu do informacji, które nie są istotne, w szczególności nie dotyczą ogłoszenia o zamówieniu, dokumentów zamówienia lub ofert.
3. Oświadczenia i dokumenty przekazywane za pośrednictwem poczty elektronicznej nie będą uwzględniane i rozpatrywane.
4. Zaleca się, aby korespondencję kierowaną do Zamawiającego opatrzyć numerem referencyjnym sprawy, tj.: DOA.201.2.2026.

## XII. Termin związania ofertą

1. Wykonawca pozostanie związany złożoną przez siebie ofertą do dnia 30.04.2026 r.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w pkt. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

## XIII. Opis sposobu przygotowania oferty

1. Zgodnie z art. 218 ust. 1 Pzp Wykonawca może złożyć jedną ofertę. Oferty Wykonawcy, który złoży więcej niż jedną ofertę, zostaną uznane za niezgodne z Pzp i odrzucone na podstawie art. 226 ust. 1 pkt 3 Pzp.
2. Treść oferty musi być zgodna z wymaganiami Zamawiającego określonymi w SWZ z załącznikami. Wykonawca zobowiązany jest do złożenia oferty, której treść pozwoli Zamawiającemu na jej zweryfikowanie pod względem zgodności z wymaganiami określonymi w SWZ z załącznikami.
3. Oferta wraz z załącznikami musi być sporządzona przez Wykonawcę ściśle według postanowień SWZ. Oferta oraz pozostałe oświadczenia i dokumenty, dla których określone zostały przez Zamawiającego w załącznikach do SWZ wzory formularzy, powinny być sporządzone zgodnie z tymi wzorami, wypełnione przez Wykonawcę według tych wzorów, zgodnie z treścią postanowień zawartych w SWZ. Wykonawca może wprowadzić modyfikacje układu graficznego

we wzorze wypełnianych dokumentów, ale treść wzoru dokumentów musi pozostać niezmienną. W przypadku gdy jakiś fragment treści wzoru nie dotyczy Wykonawcy, należy postąpić zgodnie z instrukcją wypełniania załącznika lub wpisać: „nie dotyczy”.

4. Oferta musi być sporządzona w języku polskim.
5. Wykonawca przygotowuje ofertę przy pomocy Interaktywnego formularza ofertowego udostępnionego przez Zamawiającego na Platformie e-Zamówienia i zamieszczonego w podglądzie postępowania w zakładce „Informacje podstawowe”.
6. Zalogowany Wykonawca używając przycisku „Wypełnij” widocznego pod „Formularzem ofertowym”, o którym mowa w pkt. 5, zobowiązany jest do zweryfikowania poprawności danych automatycznie pobranych przez system z jego konta i uzupełnienia pozostałych informacji dotyczących Wykonawcy/Wykonawców wspólnie ubiegających się o udzielenie zamówienia.
7. Następnie Wykonawca powinien pobrać „Formularz ofertowy”, zapisać go na dysku komputera użytkownika, uzupełnić pozostałymi danymi wymaganymi przez Zamawiającego i ponownie zapisać na dysku komputera użytkownika oraz podpisać odpowiednim rodzajem podpisu elektronicznego.
8. **Uwaga! Nie wolno zmieniać nazwy pliku nadanej przez Platformę e-Zamówienia! Zapisany „Formularz ofertowy” należy zawsze otwierać w programie Adobe Acrobat Reader DC.**
9. Wykonawca składa ofertę za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania, po zalogowaniu się na konto Wykonawcy. Po wybraniu przycisku „Złóż ofertę” system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola typu „drag&drop” (przeciągnij i upuść) służące do dodawania plików.
10. Wykonawca dodaje z dysku podpisany „Formularz ofertowy”, o którym mowa w pkt 5, w pierwszym polu („Wypełniony formularz oferty”). W kolejnym polu („Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”) Wykonawca dodaje pozostałe pliki stanowiące ofertę lub składane wraz z ofertą.
11. Interaktywny Formularz ofertowy **składa się, pod rygorem nieważności, w formie elektronicznej (opatrzonej podpisem kwalifikowanym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.**
12. **Pozostałe dokumenty** wchodzące w skład oferty lub składane wraz z ofertą, mogą być zgodnie z wyborem Wykonawcy opatrzone podpisem, o którym mowa w pkt. 11, typu zewnętrznego lub wewnętrznego. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę” dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).

13. Podpisy kwalifikowane wykorzystywane przez Wykonawców do podpisywania wszelkich plików muszą spełniać wymogi „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku”.
14. W przypadku przekazywania dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
15. Do oferty należy dołączyć ankietę bezpieczeństwa, wypełniony formularz cenowy oraz oświadczenie o niepodleganiu wykluczeniu i spełnieniu warunków udziału w postępowaniu w zakresie wskazanym w załączniku nr 3, załączniku nr 4 oraz załączniku nr 5 do SWZ w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, a następnie zaszyfrować wraz z plikami stanowiącymi ofertę.
16. Zamawiający rekomenduje przesyłanie danych w formatach .doc, .odt, .ods, .docx, .txt, .xls, .xlsx, .pdf, .jpg, .png, ze szczególnym uwzględnieniem plików .pdf
17. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów zalecanych przez Platformę.
18. Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, Zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.
19. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
20. Zamawiający zaleca, aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
21. System sprawdza, czy złożone pliki są podpisane i automatycznie je szyfruje, jednocześnie informując o tym Wykonawcę. Potwierdzenie czasu przekazania i odbioru oferty znajduje się w Elektronicznym Potwierdzeniu Przesłania (EPP) i Elektronicznym Potwierdzeniu Odebrania (EPO). EPP i EPO dostępne są dla zalogowanego Wykonawcy w zakładce „Oferty/Wnioski”.
22. Maksymalny łączny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250 MB.
- 23. Dokumenty, które należy złożyć:**
- 1) Oferta – Interaktywny formularz ofertowy wypełniony za pośrednictwem Platformy e-Zamówienia;

- 2) Pozostałe dokumenty składane wraz z ofertą:
- a. Przedmiotowy środek dowodowy w postaci wypełnionej tabeli – Ankieta bezpieczeństwa – załącznik nr 3 do SWZ;
  - b. Formularz cenowy – załącznik nr 4 do SWZ;
  - c. Oświadczenie o braku podstaw do wykluczenia i spełnienia warunków udziału w postępowaniu, załącznik nr 5 do SWZ – w przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie o niepoleganiu wykluczeniu składa każdy z Wykonawców;
  - d. Pełnomocnictwo upoważniające do złożenia oferty, o ile ofertę składa pełnomocnik;
  - e. Pełnomocnictwo dla pełnomocnika do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia.
24. W przypadku wspólnego ubiegania się o udzielenie zamówienia, Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy.
25. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (tj. w formie elektronicznej lub postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym). Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 § 2 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie (Dz. U. z 2024 r. poz. 1001 ze zm.), które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez uppełnomocnionego.
26. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.
27. Jeżeli wraz z ofertą składane są dokumenty zawierające tajemnicę przedsiębiorstwa, Wykonawca, w celu utrzymania w poufności tych informacji,



przekazuje je w wydzielonym i odpowiednio oznaczonym pliku wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”. Zarówno załącznik stanowiący tajemnicę przedsiębiorstwa jak i uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa należy dodać w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.

28. Wykonawca może przed upływem terminu składania ofert wycofać ofertę. Wykonawca wycofuje ofertę w zakładce „Oferty/wnioski” używając przycisku „Wycofaj ofertę”.

#### XIV. Sposób oraz termin składania ofert

Ofertę należy złożyć w systemie pod adresem <https://ezamowienia.gov.pl/mp-client/tenders/ocds-148610-c063628b-9e6c-49c1-9288-6f4cdeff5895> do dnia 01.04.2026 r. do godziny 10:00.

#### XV. Termin otwarcia ofert

1. Otwarcie ofert nastąpi w trybie art. 222 Pzp w dniu 01.04.2026 r., o godzinie 10:30 za pośrednictwem Platformy.
2. W przypadku awarii Platformy, która spowoduje brak możliwości otwarcia ofert ww. terminie, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
3. Zamawiający najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Otwarcie ofert następuje poprzez użycie mechanizmu do odszyfrowywania ofert dostępnego na Platformie.
5. Informacja z otwarcia ofert opublikowana zostanie na stronie internetowej prowadzonego postępowania.
6. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

#### XVI. Podstawy wykluczenia

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie art. 108 ust. 1 oraz art. 109 ust. 1 pkt 4, 8 Pzp oraz nie podlegają wykluczeniu z postępowania na podstawie art. 1 pkt 23 rozporządzenia 2022/576 do rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1) oraz 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 (Dz. U. z 2025 r., poz. 514).
2. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.



## XVII. Warunki udziału w postępowaniu

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu, oraz spełniają nm. warunki udziału w postępowaniu dotyczące:
  - 1) zdolności do występowania w obrocie gospodarczym
    - Zamawiający nie określa warunku w tym zakresie.
  - 2) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów
    - Zamawiający nie określa warunku w tym zakresie.
  - 3) sytuacji ekonomicznej lub finansowej
    - Zamawiający nie określa warunku w tym zakresie.
  - 4) zdolności technicznej lub zawodowej
    - a. Wykonawca spełni warunek, jeżeli wykaże, że należycie wykonał, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, co najmniej jedno zamówienie – usługę świadczoną dla jednostki sektora finansów publicznych, posiadającej co najmniej 300 hostów, w szczególności polegającą na monitorowaniu systemów EDR/XDR oraz systemów SIEM, trwającą nie krócej niż 12 miesięcy.

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, warunek określony powyżej ma zostać spełniony przez jednego z Wykonawców samodzielnie.
    - b. dysponuje osobami, które skieruje do realizacji zamówienia:
      - a) Zamawiający wymaga, aby Wykonawca posiadał wykwalifikowaną kadrę w liczbie nie mniejszej niż 15 osób z poniżej wymienionymi aktualnymi certyfikatami (lub równoważnymi):
        - w zakresie praktycznej znajomości taktyk i technik ataków: CRTP (Certified Red Team Professional wydany przez Altered Security ) lub OSCP (Offensive Security Certified Professional wydany przez OffSec) lub PNTP (Professional Network Penetration Tester, wydany przez TCM Security Academy);
        - w zakresie znajomości narzędzi i technik analizy incydentów: SC-200 (Microsoft Certified Security Operations Analyst lub CDCP (Cyber Defense Certified Professional wydany przez Level Effect) lub OSIR (OffSec Incident Responder wydany przez OffSec) lub CDSA (Certified Defensive Security Analyst wydany przez HTB Academy);
      - b) Zamawiający wymaga, aby zespół Wykonawcy dysponował, co najmniej jedną osobą z certyfikatem audytora wiodącego ISO27001 (lub równoważny);
      - c) Zamawiający wymaga, aby zespół Wykonawcy dysponował, co najmniej dwoma osobami, których kompetencje będą potwierdzone co

najmniej certyfikatem Microsoft AZ-500 (Microsoft Certified Azure Security Engineer) (lub równoważny);

- d) Zamawiający wymaga, aby zespół Wykonawcy dysponował inżynierami, których kompetencje są potwierdzone stosownymi certyfikatami producentów;
- e) Zamawiający wymaga, aby wszystkie osoby obsługujące SOC, które będą się komunikować z Zamawiającym posługiwały się w mowie i piśmie językiem polskim na poziomie biegłym.

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, warunki określone powyżej mogą zostać spełnione przez jednego z Wykonawców lub wspólnie.

- 2. Wykonawca może, na zasadach określonych w art. 118 ustawy Pzp, w celu potwierdzenia spełniania warunków udziału w postępowaniu lub kryteriów selekcji, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
- 3. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów. Zobowiązanie (lub inny dokument) potwierdzające udostępnianie zasobów przez inne podmioty należy złożyć wraz z ofertą.
- 4. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w pkt. 3 potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
  - 1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
  - 2) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
  - 3) czy i w jakim zakresie podmiot udostępniający zasoby na zdolnościach, którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.

5. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
6. W celu wykazania braku podstaw wykluczenia oraz spełnienia warunków udziału w postępowaniu Zamawiający żąda złożenia oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp.
7. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp, innych dokumentów lub oświadczeń składanych w postępowaniu w celu wykazania warunków udziału w postępowaniu lub braku podstaw do wykluczenia Wykonawcy lub są one niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w terminie przez siebie wskazanym, chyba że oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie, lub zachodzą przesłanki unieważnienia postępowania.

## XVIII. Wykaz podmiotowych środków dowodowych

1. Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia niżej wymienionych podmiotowych środków dowodowych:
  - 1) Wykaz usług (minimum jednej usługi) wykonanych, a w przypadku powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy w tym okresie, wykonał lub wykonuje należycie, co najmniej usługę świadczoną dla jednostki sektora finansów publicznych, posiadającej co najmniej 300 hostów, w szczególności polegającą na monitorowaniu systemów EDR/XDR oraz systemów SIEM, trwającą nie krócej niż 12 miesięcy. Dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były lub są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy. Wzór wykazu usługi stanowi załącznik nr 6 do SWZ.
  - 2) Wykaz osób, o których mowa w Rozdziale XVII pkt 1 ppkt 4) lit. b. SWZ, skierowanych przez Wykonawcę do realizacji zamówienia wraz z informacją dotyczącą roli w realizacji zamówienia, zakresu wykonywanych przez nie zadań/czynności, z wyszczególnieniem posiadanych certyfikatów, przeszkoleń oraz podstawie dysponowania tymi osobami. Wzór wykazu osób stanowi załącznik nr 7 do SWZ.
2. W zakresie nieuregulowanym w SWZ, zastosowanie mają postanowienia:
  - 1) Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych

dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy;

- 2) Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie.

## XIX. Sposób obliczenia ceny

1. W Interaktywnym formularzu ofertowym, wypełnianym za pośrednictwem Platformy, Wykonawca podaje cenę brutto oferty za wykonanie przedmiotu zamówienia. Cena brutto oferty podana w Interaktywnym formularzu oferty powinna być równa wartości brutto podanej przez Wykonawcę w Formularzu cenowym – załącznik nr 4 do SWZ.
2. W przypadku rozbieżności pomiędzy ceną wskazaną w Formularzu ofertowym podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena podana słownie.
3. Ceny poszczególnych elementów zamówienia (wartości brutto, netto i podatku VAT) wskazane zostaną przez Wykonawcę w Formularzu cenowym, którego wzór stanowi załącznik nr 4 do SWZ.
4. W przypadku rozbieżności całkowitej ceny brutto oferty podanej w Interaktywnym formularzu ofertowym a Formularzu cenowym za właściwą zostanie przyjęta cena podana w Formularzu cenowym.
5. W przypadku rozbieżności pomiędzy cenami brutto wskazanymi przez Wykonawcę w Formularzu cenowym a wynikiem sumowania cen netto i wartości podatku VAT dokonanego przez Zamawiającego, za właściwe zostaną uznane ceny wynikające z wyliczenia z cen netto i wartości podatku vat.
6. Cenę oferty należy określić w oparciu o Projektowane postanowienia umowy stanowiące załącznik nr 1 do SWZ oraz Opis przedmiotu zamówienia stanowiący załącznik nr 2 do SWZ.
7. Wykonawca podaje cenę oferty, która uwzględnia całkowity koszt realizacji zamówienia. Cena oferty musi zawierać wszelkie koszty niezbędne do zrealizowania zamówienia wynikające wprost z opisu przedmiotu zamówienia, jak również w nim nie ujęte, a bez których nie można realizować zamówienia. Oferta musi zawierać ostateczną, sumaryczną cenę obejmującą wszystkie koszty z uwzględnieniem wszystkich opłat i podatków (także podatku od towarów i usług), a także ewentualne upusty i rabaty zastosowane przez Wykonawcę.
8. Cena musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.

9. Wykonawca zobowiązany jest zastosować stawkę VAT zgodnie z obowiązującymi przepisami ustawy z 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2025 r. poz. 775 ze zm.).

## XX. Opis kryteriów oceny ofert, wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy ocenie ofert Zamawiający będzie się kierował kryterium przedstawionym poniżej:

Lp.	Kryterium oceny	Waga kryterium
1	Cena brutto wykonania przedmiotu zamówienia	100 pkt

2. Punkty przyznawane za podane kryterium będą liczone według następującego wzoru:

Nr kryterium	Sposób oceny ofert
1	<p>Oferta z najniższą ceną uzyska 100 punktów. Pozostałe oferty będą oceniane odpowiednio – proporcjonalnie do ceny najniższej, zgodnie z poniższym wzorem:</p> $\frac{\text{oferta z ceną najniższą}}{\text{oferta badana}} \times 100 = \text{liczba punktów}$ <p>Końcowy wynik poniższego działania zostanie zaokrąglony do dwóch miejsc po przecinku.</p>

3. Zamawiający zastosował jedyne kryterium „Cena – 100%” na podstawie art. 246 ust. 2 Pzp, ponieważ Opis przedmiotu zamówienia szczegółowo określa wymagania jakościowe dotyczące co najmniej głównych elementów usługi SOC 24/7/365. Przy tak opisanym standardzie minimalnym oferty porównywane są obiektywnie ceną.
4. Ocenie będą podlegać wyłącznie oferty niepodlegające odrzuceniu.
5. Za najkorzystniejszą zostanie uznana oferta, która nie podlega odrzuceniu i uzyska najwyższą łączną liczbę punktów w wyżej wymienionym kryterium oceny ofert.
6. Najkorzystniejsza oferta może uzyskać maksymalnie 100 pkt.
7. Wszelkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.
8. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą określonym w SWZ.
9. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający przed terminem związania ofertą, zwróci się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazany przez niego okres.
10. W przypadku braku zgody, o której mowa w pkt. 9, oferta podlega odrzuceniu na podstawie art. 226 ust. 1 pkt 12 Pzp.



## XXI. Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577 Pzp, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w pkt. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertę.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o miejscu i terminie podpisania umowy.
4. Wykonawca, o którym mowa w pkt. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w Projektowanych postanowieniach umowy, które stanowią załącznik nr 2 do SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.
5. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty jako najkorzystniejszej) przedstawiają Zamawiającemu umowę regulującą współpracę tych Wykonawców.
6. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

## XXII. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów Pzp.
2. Odwołanie przysługuje na:
  - 1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na Projektowane postanowienie umowy;
  - 2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy.
3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.
4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 Pzp, stronom oraz



uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.

5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej” Pzp.

### XXIII. Obowiązek informacyjny wynikający z art. 13 RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej „RODO”, informujemy, że:

- administratorem Pani/Pana danych osobowych jest Urząd Ochrony Danych Osobowych z siedzibą w Warszawie przy ul. Stanisława Moniuszki 1A. Może się Pani/Pan kontaktować z nim w następujący sposób - listownie na adres: ul. Stanisława Moniuszki 1A, 00-014 Warszawa lub przez elektroniczną skrzynkę podawczą na stronie <https://www.uodo.gov.pl/pl/p/kontakt> ;
- w sprawach związanych z Pani/Pana danymi osobowymi proszę kontaktować się z Inspektorem Ochrony Danych, w następujący sposób - listownie na adres: ul. Stanisława Moniuszki 1A, 00-014 Warszawa lub za pośrednictwem poczty elektronicznej pod adresem: [iod@uodo.gov.pl](mailto:iod@uodo.gov.pl) ;
- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w zw. z ustawą z dnia 11 września 2019 r. – Prawo zamówień publicznych (dalej: Pzp), w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego oraz jego rozstrzygnięcia, jak również zawarcia umowy w sprawie zamówienia publicznego oraz jej realizacji, a także udokumentowania postępowania o udzielenie zamówienia publicznego i jego archiwizacji na podstawie art. 6 ust. 1 lit. c RODO w zw. z ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach;
- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 Pzp oraz Prezes Urzędu Zamówień Publicznych z siedzibą w Warszawie (02-676) przy ul. Postępu 17A jako Administrator Danych Osobowych użytkowników Platformy e-Zamówienia, na której Urząd Ochrony Danych Osobowych prowadzi postępowania o udzielenie zamówienia publicznego, działając pod adresem <https://ezamowienia.gov.pl/pl/>;
- Pani/Pana dane osobowe w przypadku postępowań o udzielenie zamówienia publicznego będą przechowywane przez okres oznaczony kategorią archiwalną wskazaną w Jednolitym Rzeczowym Wykazie Akt Urzędu Ochrony Danych Osobowych, który zgodnie z art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach został przygotowany

w porozumieniu z Naczelnym Dyrektorem Archiwów Państwowych. Dla dokumentów wytworzonych w ramach zamówień publicznych krajowych jest to okres 5 lat. Okres przechowywania liczony jest od 1 stycznia roku następnego od daty zakończenia sprawy. Po upływie okresu przechowywania dokumentacja niearchiwalna podlega, po uzyskaniu zgody dyrektora właściwego archiwum państwowego, brakowaniu;

- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z Pzp;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
- Posiada Pan/Pani:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych, przy czym skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z Pzp oraz nie może naruszać integralności protokołu postępowania oraz jego załączników;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO, przy czym prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego, a także nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych; prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO; na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

## XXIV. Spis załączników do SWZ

Integralną częścią niniejszej SWZ stanowią następujące załączniki:

1. Opis przedmiotu zamówienia – załącznik nr 1;
2. Projektowane postanowienia umowy – załącznik nr 2;
3. Przedmiotowy środek dowodowy – Ankieta bezpieczeństwa – załącznik nr 3;
4. Formularz cenowy – załącznik nr 4;
5. Oświadczenie o niepodleganiu wykluczeniu oraz spełnieniu warunków udziału w postępowaniu – załącznik nr 5;
6. Wzór wykaz usług – załącznik nr 6;
7. Wzór wykazu osób skierowanych do realizacji zamówienia – załącznik nr 7.

## OPIS PRZEDMIOTU ZAMÓWIENIA

- I. Wymagania dla systemu EDR/XDR oferowanego w ramach SOC Security Operation Center
  1. W celu świadczenia usługi Wykonawca dostarczy, wdroży i będzie monitorował system EDR.
  2. Wykonawca zapewni objęcie zakresem usług 400 urządzeń końcowych, w tym stacji roboczych i serwerów.
  3. Oferowane rozwiązanie EDR musi być rozwiązaniem ocenianym przez Gartner jako Leader w „Magic Quadrant for Endpoint Protection Platforms”.
  4. Oferowane rozwiązanie EDR musi być rozwiązaniem, które w ostatnich testach organizacji MITRE ATT&CK 2024 Enterprise Evaluation osiągnęło rezultat detekcji na poziomie 99% we wszystkich 3 scenariuszach.
  5. System zostanie wdrożony na wszystkich wskazanych przez Zamawiającego hostach z systemami Microsoft Windows, Linux.
  6. System umożliwi realizację zadań SOC związanych z analizą zdarzeń zapewniając zbieranie, gromadzenie, analizę i prezentację danych telemetrycznych z punktów końcowych. Telemetria będzie obejmowała co najmniej następujące zdarzenia: utworzenia każdego procesu (Nazwa, ścieżka obrazu, argumenty, suma kontrolna, czas), operacji utworzenia, modyfikacja, usunięcie plików (ścieżka, suma kontrolna, nazwa procesu odpowiedzialnego, ścieżka do obrazu procesu odpowiedzialnego), interakcje między procesami (rodzaj operacji, źródło, cel, ścieżki obrazów), komunikacji TCP/IP (adresy, porty, nazwa procesu odpowiedzialnego, ścieżka do obrazu procesu odpowiedzialnego), zapytania DNS (pełna treść zapytania i odpowiedzi, nazwa procesu odpowiedzialnego, ścieżka do obrazu procesu odpowiedzialnego), uwierzytelniania (nazwa użytkownika, rodzaj, czy udane), adresy URL. Dodatkowo dla systemów Microsoft Windows, rejestrację wszystkich operacji w rejestrze niezależnie od gałęzi rejestru (dodanie, usunięcie, modyfikacja klucza rejestru lub wartości klucza, wartość przed zmianą i po zmianie), operacje dotyczące zaplanowanych zadań (dodanie, usunięcie, modyfikacja), treści uruchamianych skryptów powershell, polecenia wydane w sesjach powershell, cmd, bash, wraz z ich parametrami. Dane telemetryczne będą gromadzone dla wszystkich operacji na hostach bez względu na występujące alerty. Wszystkie dane telemetryczne będą dostępne w konsoli przez okres minimum 30 dni. Dane dotyczące detekcji będą dostępne w konsoli przez okres 12 miesięcy od momentu wdrożenia usługi. Po zakończeniu umowy Wykonawca przekaże Zamawiającemu dane z detekcji.
  7. System umożliwi realizację zadań SOC związanych z reakcją na incydenty zapewniając wykonywanie następujących działań: ekstrakcja istniejących procesów, poddawanie plików kwarantannie oraz wymuszanie miejscowej izolacji

hosta od sieci (pozostawiając komunikacja z konsolą zarządzającą). Dla systemów Windows reakcja musi umożliwiać dodatkowo usunięcie zmian wprowadzonych w rejestrach oraz przywrócenie zmodyfikowanych plików z kopii VSS. Wszystkie reakcja muszą być możliwe do podjęcia w sposób zautomatyzowany w reakcji na detekcję oraz manualny przez analityka SOC, w reakcji na zidentyfikowane incydenty, z poziomu alertu. Reakcje muszą być realizowane przez jednego agenta i nie mogą wymagać uruchamiania dodatkowych skryptów i playbooków. Rozwiązanie EDR musi zapewniać funkcjonalność zdalnego wiersza poleceń (powershell, bash).

8. Agent EDR musi mieć możliwość działania w trybie widocznym dla użytkownika oraz w trybie ukrytym, gdzie komponenty agenta pozostają niewidoczne dla użytkownika końcowego. Wykonawca musi posiadać możliwość wyświetlenia komunikatu na stacji końcowej użytkownika nawet wtedy, gdy stacja została poddana izolacji sieciowej.
9. Agent EDR musi być wyposażony w silne mechanizmy samoobrony przed nieautoryzowaną manipulacją oraz uniemożliwiające użytkownikom systemu modyfikacje stanu agenta nawet wtedy, gdy mają oni uprawnienia administratora. Modyfikacja i odinstalowanie agenta muszą wymagać unikalnego hasła. Hasło musi być indywidualne dla każdego agenta. Z poziomu konsoli musi istnieć możliwość wygenerowania nowego hasła.
10. Agent musi mieć możliwość zarządzania dostępem urządzeń peryferyjnych (USB, Bluetooth) takich jak pamięci przenośne, urządzenia multimedialne.
11. Agent musi być w pełni autonomiczny, co oznacza, że jego działanie i funkcjonalność nie może być zależna od dostępności konsoli zarządzania, chmury ani żadnych zasobów zewnętrznych od agenta. Wykrywanie i reagowanie na zaawansowane zagrożenia musi być możliwe w czasie rzeczywistym, nie może zależeć od stanu sieciowego stacji (agent musi realizować te same funkcjonalności w trybie online i offline) oraz nie może wymagać innego rodzaju zewnętrznych zasobów.
12. Rozwiązanie musi umożliwiać integrację z usługą Active Directory, aby możliwe było automatyczne przypisywanie agentów do grup, w celu powiązania ich z zasadami AD. Konsola zarządzania nie powinna łączyć się z usługą Active Directory bezpośrednio za pośrednictwem programu ADFS ani żadnej innej metody uzyskiwania atrybutów usługi AD. Serwer zarządzania rozwiązaniem nie powinien mieć żadnych zależności od stanu usługi AD.
13. EDR musi obsługiwać tworzenie dodatkowych, własnych reguł detekcji. Ta funkcjonalność ma umożliwić analitykom SOC przekształcenia zapytań do bazy telemetry w automatyczne reguły detekcji, które wyzwalają alerty i automatyczne odpowiedzi, gdy reguły wykryją zdefiniowane zachowanie stacji końcowej.
14. Rozwiązanie EDR musi umożliwiać dodawanie własnych indyktorów IoC co najmniej w zakresie adresów IP, domen, adresów URL, hashy SHA1, SHA256.



Przy dodawaniu indykatorów musi istnieć możliwość ustawienia czasu ich automatycznego wygaśnięcia.

15. Rozwiązanie EDR musi być hostowane na terenie Unii Europejskiej.

II. Wymagania dla systemu XDR/SIEM oferowanego w ramach SOC Security Operation Center

1. Funkcje systemu XDR i systemu SIEM mogą być realizowane przez jedno rozwiązanie.
2. W celu świadczenia usługi Wykonawca dostarczy, wdroży i będzie monitorował system klasy SIEM, który zapewni odbiór, normalizację (parsowanie), korelację, wyszukiwanie i wizualizację logów przesłanych z systemów Zamawiającego.
3. Licencja musi pozwalać na dostarczenie 20 GB logów dziennie.
4. System musi przechowywać dane z retencją 30 dni.
5. W przypadku dostarczenia systemu w modelu SaaS, system SIEM musi zostać dostarczony i utrzymywany (hostowany) w chmurze na terenie EU.
6. System musi zapewniać dedykowane oprogramowanie – agenta umożliwiającego gromadzenie logów z systemów operacyjnych Linux i Windows. Konfiguracja agenta musi pozwalać na określenie typów logów, które będą przesyłane do centralnego repozytorium logów.
7. System musi zapewniać możliwość bezagentowego gromadzenia logów przesłanych protokołem Syslog.
8. System musi umożliwiać wyszukiwanie danych za pomocą wbudowanego języka zapytań, w oparciu o wartości sparsowanych pól logów oraz ich wizualizację.
9. System musi umożliwiać wyszukiwanie dla dowolnych fraz łączonych wyrażeniami logicznymi.
10. System musi automatycznie grupować wyniki zapytań ze względu na najczęściej występujące pola i ich wartości. Wyniki grupowania muszą być wyświetlane w formie tabelarycznej i graficznej, wraz z informacjami statystycznymi na ich temat.
11. System musi być wyposażony w mechanizmy reguł detekcji, które automatycznie wyświetlają i sygnalizują alertami wystąpienia zdarzeń spełniających następujące warunki: wartość pola logu zgodna ze zdefiniowaną, zdefiniowana ilość wystąpień zdarzeń o określonej wartości pól w zdefiniowanym czasie, wystąpienie określonej relacji w wartościach pól między różnymi zdarzeniami.
12. System musi być wyposażony w mechanizmy prezentacji i wizualizacji alertów wygenerowanych w wyniku działania reguł detekcji w taki sposób, aby wyniki te mogły być filtrowane i grupowane z użyciem filtrów wartości pól alertów.
13. Wszystkie użytkowe funkcje systemu takie jak: wyszukiwanie i analiza danych, zarządzanie systemem, tworzenie reguł detekcji i prezentacja wyników ich działania, muszą być dostępne w graficznym interfejsie użytkownika wyświetlanym w przeglądarce WEB.



14. Zamawiający nie dopuszcza systemu SIEM opartego o licencję typu opensource.
15. Zaoferowany system SIEM musi być objęty wsparciem producenta przez cały okres trwania świadczenia usługi.

### III. Utrzymanie systemów

1. Wykonawca zapewni ciągły monitoring wydajności i dostępności monitorowanych systemów.
2. W każdym przypadku niedostępności monitorowanych systemów lub ich nieprawidłowego działania, które negatywnie wpłyną na ich możliwości pod względem gromadzenia danych oraz wykrywania i reakcji na zagrożenia, Zamawiający podejmie działania w celu rozwiązania problemu w czasie do 12 godzin od momentu wykrycia problemu przez Wykonawcę lub zgłoszenia problemu przez Zamawiającego.
3. W każdym przypadku nieprawidłowego działania monitorowanych systemów, które negatywnie wpłyną na systemy IT Zamawiającego, Wykonawca podejmie działania w celu usunięcia problemu w czasie do 6 godzin od wykrycia lub zgłoszenia problemu.
4. W każdym przypadku nieprawidłowego działania monitorowanych systemów, które uniemożliwia działanie systemów IT Zamawiającego, Wykonawca podejmie działania w celu usunięcia problemu w czasie do 2 godzin od wykrycia lub zgłoszenia problemu.
5. Wykonawca zapewni aktualność wersji oprogramowania monitorowanych systemów zgodnie z zaleceniami ich producentów.

### IV. Przyjmowanie zgłoszeń i monitoring alertów

1. Wykonawca zapewni przyjmowanie i rejestrację zgłoszeń związanych z incydentami lub podejrzeniami incydentów cyberbezpieczeństwa. Zgłoszenia mogą być dokonywane przez osoby wskazane przez Zamawiającego, za pośrednictwem ustalonych kanałów komunikacji (e-mail, telefon, komunikator internetowy). Przyjmowanie zgłoszeń musi być realizowane 24 godziny na dobę, przez personel dysponujący wiedzą i doświadczeniem w zakresie analizy incydentów cyberbezpieczeństwa.
2. Wykonawca będzie prowadził rejestr obejmujący szczegółowe informacje o zgłoszeniach z uwzględnieniem:
  - Czasu przyjęcia zgłoszenia.
  - Osób odpowiedzialnych za obsługę zgłoszenia.
  - Przebiegu i wyników przeprowadzonych analiz.
  - Historii podjętych czynności i komunikacji.
3. Wykonawca będzie informował Zamawiającego o statusie zgłoszeń zgodnie z przyjętymi ścieżkami eskalacji. Każde zgłoszenie musi być oznaczone unikalnym identyfikatorem, który zostanie przekazany osobie zgłaszającej oraz będzie

wykorzystywany w dalszej komunikacji. Rejestr zgłoszeń, wraz ze wszystkimi szczegółami dotyczącymi zgłoszeń będzie przechowywany przez cały okres trwania umowy. Zamawiający otrzyma dostęp do wyżej wymienionych informacji o każdym zgłoszeniu niezwłocznie, na każde żądanie.

4. Usługodawca będzie prowadził stały monitoring alertów i zdarzeń:
  - w systemie EDR/XDR bez ograniczeń;
  - w systemie SIEM do 30 alertów miesięcznie;
  - za pośrednictwem ustalonych kanałów komunikacji do 10 zgłoszeń miesięcznie.
5. Wykonawca zarejestruje każdy alert, który wystąpi w systemach Zamawiającego. Rejestracja alertu w systemie obsługi zgłoszeń Wykonawcy nastąpi nie później niż w czasie 10 min. od utworzenia alertu w monitorowanym systemie.
6. Wykonawca będzie prowadził rejestr obejmujący informacje o wszystkich alertach, ze szczególnym uwzględnieniem:
  - Czasu wystąpienia alertu w monitorowanym systemie;
  - Czasu zarejestrowania alertu w systemie obsługi zgłoszeń Wykonawcy;
  - Czasu rozpoczęcia analizy zdarzenia;
  - Osób zaangażowanych w proces obsługi;
  - Przebiegu i wyników analizy;
  - Klasyfikacji;
  - Historii podjętych czynności i komunikacji.
7. Każde wystąpienie alertu musi być oznaczone unikalnym identyfikatorem, który będzie wykorzystywany w dalszej komunikacji.
8. Rejestr zdarzeń, wraz ze wszystkimi szczegółami dotyczącymi alertów będzie przechowywany przez cały okres trwania umowy. Zamawiający otrzyma dostęp do wyżej wymienionych informacji o każdym zdarzeniu niezwłocznie, na każde żądanie.

## V. Analiza zdarzeń

1. Wykonawca przeprowadzi analizę każdego alertu, który wystąpi w monitorowanych systemach oraz informacji uzyskanych w wyniku zgłoszeń użytkowników. Analiza musi uwzględniać co najmniej:
  - Ustalenie dokładnego przebiegu zdarzeń na podstawie telemetrii dostępnej w monitorowanych systemach;
  - Wyodrębnianie artefaktów zdarzeń;
  - Uzupełnianie danych i kontekstu zdarzeń z wykorzystaniem źródeł Threat Intelligence Usługodawcy, OSINT, informacji dostępnych w bazie wiedzy o zasobach IT zamawiającego, informacji uzyskanych od administratorów i użytkowników, zgodnie z ustalonymi punktami kontaktowymi i ścieżkami eskalacji;

- Pivoting polegający na identyfikacji i analizie powiązań między zdarzeniami lub artefaktami pozyskanymi z systemu oraz informacjami uzyskanymi w rezultacie uzupełniania kontekstu. W tym celu musi wykorzystywać dostępne dane, takie jak adresy IP, identyfikatory użytkowników, nazwy hostów czy informacje o plikach jako punkt wyjścia do eksploracji i analizy;
  - Krzyżową weryfikację zdarzeń w monitorowanych systemach, analizę telemetrii dostępnej w systemach pod kątem zdarzeń powiązanych;
  - W przypadku zdarzeń związanych ze złośliwym lub podejrzanym oprogramowaniem, którego charakteru nie można jednoznacznie określić na podstawie źródeł Threat Intelligence lub analizy telemetrii, Wykonawca przeprowadzi dodatkowe działania, które muszą uwzględniać co najmniej: dynamiczną analizę w środowiskach sandbox Wykonawcy oraz, jeśli to konieczne, w środowisku laboratoryjnym Wykonawcy, w tym: kontrolowaną detonację, deobfuskację i inżynierię wsteczną kodu, w celu ustalenia szczegółów technicznych (IOC), technik ataku, charakteru i potencjalnych skutków uruchomienia tego oprogramowania;
  - W przypadku zdarzeń związanych z podejrzanyymi lub złośliwymi domenami adresami IP i URL działania muszą uwzględniać weryfikację tych adresów w źródłach Threat Intelligence oraz, jeśli to konieczne, bezpośrednią weryfikację ich zawartości;
  - Analizę zgromadzonych danych i sekcję zdarzeń pod kątem możliwości wystąpienia incydentów bezpieczeństwa.
2. Wykonawca zagwarantuje rozpoczęcie analizy każdego alertu w czasie nie dłuższym niż dwie godziny od jego wystąpienia w systemie Zamawiającego.
  3. Wykonawca zapewni nieprzerwaną analizę od momentu rozpoczęcia do ustalenia charakteru zdarzenia.
  4. Analiza każdego alertu musi być zakończona klasyfikacją zgodnie z ustaloną taksonomią klasyfikacji. Klasyfikacja musi uwzględniać co najmniej charakter zdarzenia (True-Positive, False-positive, Benign True-Positive) i musi wynikać z przeprowadzonej analizy.
  5. Wykonawca nie może zakończyć ani przerwać analizy, dopóki nie będzie możliwe sklasyfikowanie zdarzenia.
  6. Każda analiza musi być potwierdzona raportem, w którym analityk opíše ustalenia będące podstawą do klasyfikacji.
  7. Dla każdego przeanalizowanego zgłoszenia i alertu Wykonawca dostarczy raport z analizy uwzględniający co najmniej:
    - Dokładny czas wystąpienia alertu w monitorowanym systemie;
    - Dokładny czas rejestracji zdarzenia w systemie obsługi zgłoszeń Zamawiającego;
    - Dokładny czas rozpoczęcia i zakończenia analizy;
    - Opis analizy z uwzględnieniem prowadzonych działań;

- Zgromadzone i przeanalizowane artefakty;
- Rezultat analizy i klasyfikację;
- Rekomendacje;
- Zawarte w raporcie rekomendacje, rezultaty analizy i klasyfikacje muszą wynikać z analizy.

## VI. Raportowania i spotkania operacyjne

1. Raz w miesiącu, w ustalonym terminie, Wykonawca prześle Zamawiającemu raport zawierający co najmniej:
  - Informacje zbiorcze na temat ilości przeprowadzonych analiz;
  - Informacje na temat klasyfikacji wynikających z analiz;
  - Zestawienie typów występujących alertów i incydentów;
  - Zestawienie priorytetów alertów i incydentów;
  - Średni czas reakcji;
  - Średni czas obsługi;
  - Zestawienie najważniejszych rekomendacji;
  - Informacje na temat stanu (wydajności, obciążenia, problemów) monitorowanych systemów bezpieczeństwa.
2. Raz w miesiącu Wykonawca zapewni spotkanie operacyjne w celu omówienia procedur, ścieżek eskalacji, konfiguracji monitorowanych systemów, parametrów usługi, zaleceń. Spotkania będą odbywały się w siedzibie Zamawiającego lub za zgodą Zamawiającego, on-line.

## VII. Zarządzanie systemami i optymalizacja mechanizmów detekcji

1. Wykonawca zapewni zarządzanie konfiguracją monitorowanych systemów zgodnie z ustalonym procesem wprowadzania zmian oraz w ramach ustalonej autoryzacji i poziomów dostępu w zakresie tuningu reguł detekcji, w celu podniesienia efektywności wykrywania zagrożeń i redukcji ilości fałszywych alarmów.
2. Dla powtarzających się alertów, których analiza wykazała, że są fałszywymi alarmami Wykonawca przeprowadzi analizę mechanizmów detekcji, zaproponuje i wprowadzi zmiany w celu ograniczenia ilości fałszywych alarmów. Zmiany będą wprowadzane zgodnie z ustaloną autoryzacją i procesem wprowadzania zmian.
3. Dla wszystkich alertów, których analiza wykaże, że są fałszywymi alarmami oraz że w ich wyniku wyzwolone zostały automatyczne mechanizmy reakcji, które zakłócają działanie systemów IT Zamawiającego, Wykonawca w ramach reakcji na wykrycie takiego zdarzenia, niezwłocznie po jego wykryciu przeanalizuje mechanizmy detekcji, zaproponuje i wprowadzi zmiany w celu wyeliminowania takich fałszywych alarmów i niepożądanego reakcji systemów bezpieczeństwa.

4. Wykonawca będzie rekomendował zmiany w konfiguracji mechanizmów detekcji monitorowanych systemów bezpieczeństwa w celu podnoszenia efektywności ochrony oraz zminimalizowania ilości fałszywych alarmów.
5. Na żądanie Zamawiającego, Wykonawca zaimplementuje zamiany w konfiguracji reguł detekcji monitorowanych systemów w celu podniesienia ich efektywności oraz ograniczenia ilości fałszywych alarmów.
6. Wykonawca będzie przyjmował zgłoszenia o nieprawidłowym działaniu monitorowanych systemów bezpieczeństwa. Każde nieprawidłowe działanie systemu będzie poddane analizie przez zespół Wykonawcy. Wykonawca podejmie działania w celu rozwiązania problemu, a jeśli to konieczne skontaktuje się z producentem systemu, będzie prowadził korespondencję i wdrażał zalecenia.
7. Wykonawca będzie przeprowadzał aktualizacje monitorowanych systemów zgodnie z zaleceniami producentów.
8. Wykonawca będzie pozyskiwał i utrzymywał aktualną bazę wiedzy o zasobach i architekturze sieci Zamawiającego na poziomie umożliwiającym określenie roli, typu oraz priorytetu zasobów. Informacje te będą wykorzystywane w procesach analizy zdarzeń i reakcji na incydenty w celu ograniczenia zaangażowania zamawiającego w te procesy.
9. Wykonawca umożliwi wskazanym przedstawicielom Zamawiającego przeprowadzenie niezapowiedzianych wizyt kontrolnych w pomieszczeniu, w którym wykonywane będą prace na rzecz Zamawiającego nie częściej niż raz na kwartał.
10. Wykonawca dostarczy listę członków zespołu zaangażowanego w świadczenie usługi.
11. Dostęp do systemów Zamawiającego oraz systemów wykorzystywanych przez Wykonawcę do świadczenia usług na rzecz Zamawiającego mogą mieć jedynie osoby uwzględnione na liście.
12. Każda zmiana w składzie zespołu świadczącego usługę musi być niezwłocznie zgłaszana Zamawiającemu.
13. Każdorazowy dostęp osób/podmiotów trzecich do systemów Zamawiającego oraz systemów wykorzystywanych przez Wykonawcę do świadczenia usług na rzecz Zamawiającego może odbywać się jedynie w pomieszczeniu wskazanym przez Wykonawcę jako miejsce świadczenia usługi oraz w obecności przedstawicieli Wykonawcy.
14. Usługa, w pełnym zakresie, musi być świadczona w trybie 24/7/365.

#### VIII. Integracje źródeł danych i systemów bezpieczeństwa

1. Wykonawca zapewni konsultacje, wsparcie techniczne i programistyczne dla prac związanych z integracją systemów bezpieczeństwa i przetwarzaniem danych będących przedmiotem lub stanowiących kontekst działań związanych z



wykrywaniem, analizą i reakcją na incydenty cyberbezpieczeństwa w następującym zakresie:

- 1.1. Automatyzacja pobierania, aktualizacji i wzbogacania danych za pośrednictwem interfejsów API dostępnych w systemach bezpieczeństwa.
- 1.2. Opracowanie i implementacja mechanizmów pobierania i normalizacja danych w systemach do analizy zdarzeń bezpieczeństwa.
- 1.3. Integracje narzędzi bezpieczeństwa z innymi systemami
- 1.4. Dokumentacja integracji.
- 1.5. Utrzymanie integracji.
2. Zadania integracji źródeł danych i systemów bezpieczeństwa będą realizowane przez Wykonawcę w wymiarze do dwóch dni roboczych, w każdym miesiącu świadczenia usługi.

IX. Wymagania w zakresie Zespołu świadczącego usługę

1. W zakresie monitoringu systemów bezpieczeństwa, analizy zdarzeń i incydentów oraz reakcji na incydenty Wykonawca będzie dysponował wykwalifikowaną kadrą w liczbie nie mniejszej niż 15 osób, która umożliwi realizację przedmiotu zamówienia.
2. Zamawiający ma świadomość złożoności i zaawansowania współczesnych ataków cybernetycznych dlatego oczekuje, żeby wszyscy członkowie zespołu realizującego monitoring systemów, analizę zdarzeń oraz reakcję na incydenty będą legitymowali się wiedzą praktyczną w zakresie cyberbezpieczeństwa, która jest potwierdzona następującymi lub równoważnymi certyfikatami branżowymi, ważnymi przez cały okres umowy.
  - 2.1. W zakresie praktycznej znajomości taktyk i technik ataków Zamawiający wymaga, aby każdy członek zespołu dysponował aktualnymi certyfikatami: CRTP (Certified Red Team Professional wydany przez Altered Security ) lub OSCP (Offensive Security Certified Professional wydany przez OffSec) lub PNTP (Professional Network Penetration Tester, wydany przez TCM Security Academy).
  - 2.2. W zakresie znajomości narzędzi i technik analizy incydentów Zamawiający wymaga, aby każdy członek zespołu musi dysponować aktualnymi certyfikatami: SC-200 (Microsoft Certified Security Operations Analyst lub CDCP (Cyber Defense Certified Professional wydany przez Level Effect) lub OSIR (OffSec Incident Responder wydany przez OffSec) lub CDSA (Certified Defensive Security Analyst wydany przez HTB Academy).
3. Zamawiający wymaga wsparcia w zakresie zgodności z normami bezpieczeństwa informacji. Dlatego zespół musi dysponować co najmniej jedną osobą dysponującą certyfikatem audytora wiodącego ISO27001 przez cały okres umowy.



4. Zamawiający wymaga wsparcia w zakresie środowisk chmurowych Microsoft. Dlatego Zespół musi dysponować co najmniej dwoma osobami, których kompetencje będą potwierdzone co najmniej certyfikatem Microsoft AZ-500 (Microsoft Certified Azure Security Engineer) przez cały okres umowy.
5. Zamawiający wymaga wsparcia technicznego w zakresie monitorowanych systemów. Dlatego Wykonawca musi dysponować inżynierami, których kompetencje są potwierdzone stosownymi certyfikatami producentów.
6. Zamawiający wymaga, aby wszystkie osoby obsługujące SOC, które będą się komunikować z Zamawiającym posługiwały się w mowie i piśmie językiem polskim na poziomie biegłym.

X. Wymagania dla Wykonawcy

1. Wykonawca musi dysponować certyfikatem ISO27001 oraz ISO22301 co najmniej w zakresie obsługi zgłoszeń i reakcji na incydenty bezpieczeństwa przez cały okres umowy.
2. Wykonawca musi utrzymywać przez cały okres umowy środowisko SOC spełniające wymagania KRI, KSC oraz RODO.
3. Wykonawca musi utrzymywać przez cały okres umowy możliwość świadczenia usług 24/7/365.
4. Wykonawca musi realizować wszystkie opisane w wymaganiach zadania na rzecz Zamawiającego korzystając z zasobów usytuowanych na terenie Unii Europejskiej.
5. Wykonawca musi udokumentować posiadane doświadczenie w zakresie realizacji usługi SOC trwającej nie krócej niż 12 miesięcy (w okresie ostatnich 3 lat), na rzecz centralnych lub terenowych urzędów administracji rządowej posiadających co najmniej 300 hostów, w szczególności polegającej na monitorowaniu systemów EDR/XDR oraz systemów SIEM.
6. Wykonawca przez cały okres trwania umowy jest zobowiązany posiadać ubezpieczenie odpowiedzialności cywilnoprawnej za szkody wyrządzone w związku z prowadzeniem działalności, na sumę ubezpieczenia nie niższą, niż 3 000 000 zł (trzy miliony złotych).

Załącznik nr 2 do SWZ

**UMOWA nr UODO/[•]/2026**

pomiędzy:

**Urzędem Ochrony Danych Osobowych**, zwanym dalej Zamawiającym, z siedzibą w Warszawie przy ul. Stanisława Moniuszki 1A, NIP 526-21-94-433, REGON 013049097, reprezentowanym przez:

.....

a

....., zwanym dalej Wykonawcą, z siedzibą w .....  
przy ....., NIP ....., REGON .....,  
reprezentowanym przez:

.....

zwanymi dalej pojedynczo „Stroną”, a łącznie „Stronami”,

Umowa została zawarta w wyniku przeprowadzonego postępowania w trybie podstawowym na podstawie art. 275 pkt 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320 ze zm), zwanej dalej Pzp, w przedmiocie: „Usługa SOC (Security Operation Center)”, w ramach realizacji Programu Cyberbezpieczny Rząd na podstawie Porozumienia o powierzenie grantu o numerze KPOD.05.10-CR.01-001/24/0050/KPOD.05.10-CR.01-001/25/2025.

**§1 Definicje**

Pojęcia użyte w treści niniejszej Umowy mają znaczenie nadane im poniżej.

1. Zdarzenie – wymagające dalszej analizy dane i informacje, których źródłem są systemy bezpieczeństwa, prezentowane w formie charakterystycznej dla tych systemów, mogące świadczyć o wystąpieniu Incydentu bezpieczeństwa lub stanowiące kontekst innych Zdarzeń powiązanych z Incydentem bezpieczeństwa.
2. Artefakt Zdarzenia / Incydentu – dane określające techniczne i behawioralne cechy Zdarzeń oraz Incydentów. Na przykład: suma kontrolna pliku (MD5, SHA1, SHA256), nazwa pliku, ścieżka pliku, typ pliku, gałąź i wartość rejestru, adres IP (źródłowy i docelowy), protokół sieciowy, aplikacja sieciowa, port sieciowy, domena, URL, dostęp do zasobu c\$.
3. Alert / Wskaźnik Incydentu – zdarzenia, których źródłem są systemy bezpieczeństwa lub zgłoszenie użytkowników, których cechy (priorytet, opis,

źródło, zasób) świadczą o możliwości wystąpienia Incydentu. Na przykład: Alert systemu EDR/NDR o wysokim priorytecie, którego opis oraz artefakty wskazują na wystąpienie Incydentu bezpieczeństwa.

4. Incydynty Cyberbezpieczeństwa – zdarzenia w systemach bezpieczeństwa, które świadczą o wystąpieniu okoliczności stanowiących zagrożenie dla systemów organizacji, danych przetwarzanych w tych systemach oraz stanowiących naruszenie polityk bezpieczeństwa, które wynikają ze złośliwych intencji.
5. Fałszywy Alarm – zdarzenia w systemach bezpieczeństwa, które nie stanowią bezpośredniego zagrożenia dla organizacji oraz wynikają z błędnego działania systemu lub celowego i autoryzowanego zaalarmowania aktywności.
6. Security Issue – zdarzenie w systemach bezpieczeństwa, które nie stanowi bezpośredniego zagrożenia dla organizacji, lecz stan, który sygnalizuje, zwiększa potencjalne ryzyko wystąpienia Incydentu.
7. Proces Obsługi Incydentu – zbiór działań realizowanych od wystąpienia Wskaźnika Incydentu do zakończenia reakcji na Incydent. Działania te zwykle obejmują: monitoring systemów, obsługę zgłoszeń, analizę i selekcję Zdarzeń oraz reakcję na Incydynty, na którą składają się najczęściej: analiza Incydentu, powstrzymanie Incydentu, zażegnanie zagrożenia, konsultacje przy przywróceniu systemów przez Zamawiającego, wyciąganie wniosków, raportowanie.
8. Czas Reakcji – czas, który upłynął od momentu rejestracji Zdarzenia w systemie obsługi zgłoszeń, lub odebrania zgłoszenia o wystąpieniu Zdarzenia od użytkownika do momentu podjęcia działań związanych z analizą i selekcją Zdarzeń.
9. Pivoting – proces wzbogacania listy artefaktów Zdarzenia bądź Incydentu o kolejne artefakty na podstawie informacji pozyskanych z dodatkowych źródeł informacji (TI, OSINT, systemów i użytkowników). W trakcie analizy Zdarzeń i Incydentów analitycy Wykonawcy dokonują krzyżowej weryfikacji występowania artefaktów w dostępnych źródłach danych. Rozszerzona lista artefaktów pomaga w potwierdzeniu bądź zaprzeczeniu wystąpienia Incydentu bezpieczeństwa w procesie analizy i selekcji Zdarzeń. W trakcie analizy Zdarzeń lub Incydentów artefakty pomagają w ustaleniu skali, wpływu oraz szczegółów technicznych Zdarzenia lub Incydentu.
10. Osoba kontaktowa (PoC) – osoba wskazana przez Zamawiającego do komunikacji z Wykonawcą w zakresie procesu obsługi Incydentów. Utrzymanie aktualnej listy kontaktów oraz ich dostępności ma krytyczny wpływ na skuteczność procesu obsługi Incydentów.
11. Ścieżka eskalacji – uzgodnione i sformalizowane zasady komunikacji w zakresie procesu obsługi Incydentów, które definiują w szczególności: dostępne kanały komunikacji, kolejność powiadamiania osób kontaktowych, kolejność i sposoby eskalacji w przypadku braku możliwości nawiązania kontaktu lub w przypadku braku reakcji.

12. Autoryzacja – uzgodniony i sformalizowany zakres działań aktywnych i proaktywnych, które Wykonawca może podjąć w ramach procesu obsługi Incydentów. Autoryzacja może uwzględniać konieczność uzyskania zgody na podjęcie działań od wskazanych osób kontaktowych, zgodnie z przyjętymi Ścieżkami eskalacji.
13. Poziom dostępu – uzgodniony i sformalizowany poziom uprawnień, którymi dysponuje Wykonawca w Ustalonych Systemach Bezpieczeństwa, niemniejszy niż niezbędny do realizowania zadań obsługi Incydentów zgodnie z przyznaną autoryzacją.
14. Cyber Threat Intelligence (CTI) – ciągły proces zbierania, analizowania i interpretowania danych o zagrożeniach cybernetycznych, w celu zidentyfikowania potencjalnych zagrożeń dla organizacji. CTI dostarcza informacji, które pomagają zrozumieć motyw, techniki oraz cele atakujących, co umożliwia skuteczniejsze zapobieganie, wykrywanie i reagowanie na Incydenty cyberbezpieczeństwa.
15. Threat Hunting – aktywne poszukiwanie zagrożeń w teledzieleniu zgromadzonej w monitorowanych systemach, w oparciu o informacje pozyskane w procesie Cyber Threat Intelligence.
16. Detection Engineering – w wyniku działania procesów Cyber Threat Intelligence oraz Threat Huntingu są tworzone detekcje wzbogacające natywne mechanizmy systemów bezpieczeństwa, skierowane na wykrywanie najnowszych zagrożeń.
17. System obsługi zgłoszeń – element platformy Wykonawcy, w którym analitycy zespołu prowadzą rejestr prac wykonywanych w ramach procesu obsługi Incydentów. Podstawowym obiektem systemu są zgłoszenia. Zgłoszenia powstają automatycznie lub są zakładane manualnie niezwłocznie po zaobserwowaniu Wskaźnika Incydentu, powiadomienia od użytkownika lub w wyniku prac Threat Hunting. Każde zgłoszenie zawiera podstawowe informacje o Zdarzeniu: źródło, opis, status, priorytet, typ Zdarzenia, czas powstania. W miarę postępu prac informacje te są uzupełniane o dane uzyskane w rezultacie analizy. Każda zmiana w zgłoszeniu jest rejestrowana i opatrzona znacznikiem czasowym oraz nazwą użytkownika. Wszystkie zgłoszenia dotyczące jednego klienta są przetwarzane w ramach dedykowanej kolejki zgłoszeń. Kolejka to zestaw parametrów konfiguracji systemu obejmujący cechy indywidualne procesu obsługi Incydentów Zamawiającego, w szczególności: wymagane pola i wartości, wymagane czasy reakcji, osoby kontaktowe, uprawnienia.
18. Usługa (Usługa operacyjnego centrum bezpieczeństwa Wykonawcy) – czynności operacyjne i inne świadczenia realizowane w ramach procesu obsługi Incydentów, przez dedykowany zespół analityków bezpieczeństwa, z wykorzystaniem wyspecjalizowanych narzędzi. Lista zdolności operacyjnych oraz ich parametry (autoryzacja, poziom uprawnień, ścieżki eskalacji, osoby kontaktowe) mogą być dostosowane do potrzeb Zamawiającego.

19. Spotkania operacyjne – cykliczne spotkania pomiędzy przedstawicielami zespołów operacyjnych, Zamawiającego i Wykonawcy. W ramach spotkań operacyjnych mogą być omawiane: bieżące tematy operacyjne, informacje dotyczące ostatnich zgłoszeń i Alertów, zaproponowane zmiany w ustaleniach operacyjnych. Podczas spotkań operacyjnych nie są podejmowane wiążące decyzje. Decyzje powinny być potwierdzone drogą mailową. Spotkania operacyjne nie obejmują tematów warsztatowych i konsultacyjnych.
20. Taksonomia klasyfikacji – schemat klasyfikacji obejmujący hierarchię i nazewnictwo Incydentów ze względu na priorytet oraz charakter zagrożeń i naruszeń.
21. Unikalna analiza Alertu SIEM – jest to obsługa Alertu pochodzącego z systemu SIEM wymagająca manualnej analizy przez analityka SOC. Zaangażowanie związane z wielokrotnym wystąpieniem Alertów sygnalizujących tę samą aktywność lub Alertów, których parametry pozwalają na zautomatyzowaną obsługę, jest równoważne jednej unikalnej analizie.

## **§ 2 Przedmiot Umowy**

W ramach niniejszej Umowy Wykonawca zobowiązuje się do świadczenia na rzecz Zamawiającego Usługi SOC (Security Operation Center), będącej Usługą operacyjnego centrum bezpieczeństwa, której zakres i parametry zostały zdefiniowane w § 3 i § 4.

1. W ramach wykonania Umowy Wykonawca zobowiązuje się do:
  - 1) wdrożenia usługi SOC u Zamawiającego, zgodnie z zakresem zdefiniowanym w § 3 i § 4 oraz w sposób opisany w § 5;
  - 2) świadczenia usługi SOC jako usługi (Security Operations Center as a Service) z wykorzystaniem systemu dostarczonego przez Wykonawcę
2. W ramach Umowy zostaną wdrożone systemy ujęte w § 9. Szczegółowy zakres oraz sposób realizacji usługi określa Opis Przedmiotu Zamówienia (OPZ), stanowiący Załącznik nr ..... do umowy. Dokument ten stanowi integralną część umowy i jest wiążący dla Stron. Zmiana zakresu określonego w OPZ wymaga formy pisemnej i nie może prowadzić do istotnej zmiany umowy.

## **§ 3 Zakres Usługi**

Wszystkie elementy Usługi realizowane na podstawie niniejszej Umowy są ograniczone możliwościami technicznymi systemów.

1. Obsługa zgłoszeń podejrzeń wystąpienia Incydentu cyberbezpieczeństwa w ramach centrum kontaktowego:
  - 1) Przyjmowanie i rejestracja zgłoszeń związanych z Incydentami lub podejrzeniami Incydentów cyberbezpieczeństwa. Zgłoszenia mogą być dokonywane przez osoby wskazane przez Zamawiającego za pośrednictwem kanałów komunikacji ustalonych w § 4. Przyjmowanie zgłoszeń będzie



realizowane przez personel dysponujący wiedzą i doświadczeniem w zakresie analizy Incydentów cyberbezpieczeństwa.

- 2) Prowadzenie rejestru obejmującego szczegółowe informacje o zgłoszeniach z uwzględnieniem: czasu przyjęcia zgłoszenia, osób odpowiedzialnych za obsługę zgłoszenia, przebiegu i wyników przeprowadzonych analiz, historii podjętych czynności i komunikacji. Informowanie o statusie zgłoszeń zgodnie z przyjętymi ścieżkami eskalacji. Każde zgłoszenie będzie oznaczone unikalnym identyfikatorem, który zostanie przekazany osobie zgłaszającej oraz będzie wykorzystywany w dalszej komunikacji. Rejestr zgłoszeń, wraz ze wszystkimi szczegółami dotyczącymi zgłoszeń będzie przechowywany przez cały okres trwania umowy. Zamawiający otrzyma dostęp do informacji o każdym zgłoszeniu niezwłocznie, na każde żądanie.
  - 3) Rozpoczęcie obsługi zgłoszeń nie później niż w czasie reakcji ustalonym w § 4.
2. Ciągły monitoring systemów bezpieczeństwa
- 1) Stały monitoring Alertów i Zdarzeń, występujących w systemach bezpieczeństwa ustalonych w §4 za pośrednictwem interfejsów programistycznych dostępnych w tych systemach bądź innych mechanizmów umożliwiających automatyczne pobieranie informacji przez Wykonawcę o występujących Alertach.
  - 2) Prowadzenie rejestru obejmującego informacje o Alertach ze szczególnym uwzględnieniem: czasu wystąpienia Alertu, przebiegu i wyników analizy, historii podjętych czynności i komunikacji. Informowanie o wynikach analizy zgodnie z ustalonymi ścieżkami eskalacji. Każde wystąpienie Alertu będzie oznaczone unikalnym identyfikatorem wykorzystywanym w dalszej komunikacji. Rejestr Zdarzeń, wraz ze wszystkimi szczegółami dotyczącymi Alertów będzie przechowywany przez cały okres trwania umowy. Zamawiający otrzyma dostęp do informacji o każdym Zdarzeniu niezwłocznie, na każde żądanie.
  - 3) Rozpoczęcie obsługi Alertów nie później niż w czasie reakcji ustalonym w § 4.
3. Analizę Zdarzeń i Alertów występujących w monitorowanych systemach bezpieczeństwa oraz informacji uzyskanych w wyniku zgłoszeń użytkowników.
- 1) Analiza uwzględni co najmniej: ustalenie dokładnego przebiegu Zdarzeń, wyodrębnianie artefaktów dostępnych w monitorowanym systemie, uzupełnianie danych i kontekstu Zdarzeń z wykorzystaniem źródeł Threat Intelligence, OSINT, informacji uzyskanych od administratorów i użytkowników zgodnie ze ścieżkami eskalacji, pivoting, krzyżową weryfikację Zdarzeń w monitorowanych systemach oraz innych systemach bezpieczeństwa wskazanych w § 4 oraz analizę telemetrii dostępnych w systemach pod kątem Zdarzeń powiązanych. W przypadku Zdarzeń związanych ze złośliwym lub podejrzanym oprogramowaniem działania uwzględniają dynamiczną analizę w

środowiskach sandbox oraz, jeśli to konieczne, w środowisku laboratoryjnym w celu ustalenia szczegółów technicznych (IOC), charakteru i potencjalnych skutków uruchomienia tego oprogramowania. W przypadku Zdarzeń związanych z podejrzanymi lub złośliwymi domenami adresami IP i URL działania uwzględniają weryfikację tych adresów w źródłach Threat Intelligence oraz, jeśli to konieczne, bezpośrednią weryfikację ich zawartości. Analiza zgromadzonych danych i sekcja Zdarzeń pod kątem możliwości wystąpienia Incydentów bezpieczeństwa.

- 2) Analiza zgłoszenia lub Alertu zakończy się określeniem czy jest to Incydent cyberbezpieczeństwa oraz klasyfikacją Zdarzenia zgodnie z taksonomią klasyfikacji.
- 3) Jeżeli Zdarzenie zostanie uznane za Incydent, zostanie ono obsługane zgodnie z procesem obsługi Incydentów opisanym w punkcie 4.
4. Obsługa Incydentów cyberbezpieczeństwa oraz ich raportowanie:
  - 1) Informowanie Zamawiającego zgodnie z ustalonymi ścieżkami eskalacji o wystąpieniu Incydentu lub podejrzeniu wystąpienia Incydentu, z uwzględnieniem ustalonej klasyfikacji Incydentów.
  - 2) Informowanie Zamawiającego na żądanie o postępach prac związanych z analizą Incydentów.
  - 3) Niezwłoczne przekazywanie Zamawiającemu informacji, zgodnie z uzgodnionymi ścieżkami eskalacji, o ustaleniach związanych z Incydentami o określonym poziomie krytyczności.
  - 4) Współpraca z osobami wskazanymi przez Zamawiającego w ramach obsługi Incydentów, w zakresie organizacyjnym i technicznym. W szczególności informowanie Zamawiającego o rekomendacjach dotyczących działań związanych z powstrzymaniem Incydentu oraz zalecanych środkach naprawczych.
  - 5) Podejmowanie działań zdalnie związanych z reakcją na Incydenty zgodnie z ustaloną autoryzacją oraz poziomem dostępu za pośrednictwem monitorowanych systemów, w zakresie ich możliwości technicznych.
  - 6) Koordynacja działań związanych z reakcją na Incydenty w przypadku konieczności podjęcia działań wymagających zaangażowania osób i zasobów technicznych po stronie Zamawiającego, dostawcy oraz podmiotów zewnętrznych. Zapewnienie stałego kontaktu do osoby odpowiedzialnej za koordynację działań w całym procesie reakcji na Incydent.
  - 7) Dla każdego Incydentu wykonawca, niezwłocznie i zgodnie z przyjętymi ścieżkami eskalacji, dostarczy raport uwzględniający co najmniej: dokładny czas wystąpienia Alertu / przyjęcia zgłoszenia, dokładny czas rozpoczęcia i zakończenia analizy, dokładny czas zakwalifikowania Alertu jako Incydent, opis analizy z uwzględnieniem prowadzonych działań, zgromadzone i

przeanalizowane artefakty, rezultat analizy i klasyfikację, listę działań podjętych w ramach reakcji na Incydent, rekomendacje.

#### 5. Threat Intelligence

- 1) Pozyskiwanie (ze źródeł zewnętrznych oraz na podstawie Incydentów przeanalizowanych przez Wykonawcę) analiza i dystrybucja w ramach zespołu Wykonawcy wiedzy w zakresie: działalności grup cyberprzestępczych i APT, technik, taktyk i procedur (TTP) wykorzystywanych w atakach cybernetycznych, doniesień i raportów o atakach, doniesień i raportów na temat podatności. Informacji i danych na temat narzędzi.

#### 6. Aktywne wyszukiwanie zagrożeń – Threat Hunting

- 1) Analiza indykatorów (IoC i IoA) uzyskanych ze źródeł CTI, Incydentów i symulacji pod kątem wykorzystania w procesie Detection Engineering.
- 2) Ustalanie zestawów danych i opracowywanie zapytań w celu weryfikacji możliwości wystąpienia Zdarzeń w monitorowanych środowiskach.

#### 7. Detection Engineering - Opracowywanie i implementacja w ustalonych systemach reguł detekcji, które są wynikiem aktywności podejmowanych w ramach procesów Threat Intelligence oraz Threat Hunting.

#### 8. Raportowanie okresowe

- 1) Raporty okresowe będą sporządzane za okres raportowy wskazany w § 4.
- 2) Raporty będą dostarczane do 15 dnia kolejnego okresu raportowego.
- 3) Raport będzie zawierał następujące informacje i dane: informacje zbiorcze na temat ilości przeanalizowanych Alertów i zgłoszeń, informacje na temat ilości i priorytetów wykrytych Incydentów, zestawienie typów występujących Incydentów, zestawienie priorytetów Incydentów, średni czas reakcji, średni czas obsługi, zestawienie najważniejszych rekomendacji.
- 4) Raport może uwzględniać dodatkowe elementy ustalone w ciągu miesiąca od otrzymania pierwszego raportu okresowego.
- 5) Wprowadzenie zmian oraz przygotowywanie dodatkowych elementów raportów będzie realizowane w ramach godzin konsultacji zgodnie z § 4.

#### 9. Spotkania operacyjne i opiekun techniczny.

- 1) Do kontaktów w sprawach operacyjnych dotyczących świadczonej Usługi Wykonawca wyznaczy opiekuna technicznego. Wykonawca zastrzega sobie prawo do zmiany wyznaczonego opiekuna technicznego.
- 2) Opiekun techniczny jest dostępny przez okres określony w § 4.
- 3) Opiekun techniczny jest koordynatorem ustaleń operacyjnych pomiędzy Zamawiającym a Wykonawcą.
- 4) Opiekun techniczny reprezentuje Wykonawcę podczas spotkań operacyjnych.
- 5) Spotkania operacyjne to cykliczne spotkania pomiędzy przedstawicielami zespołów operacyjnych, Zamawiającego i Wykonawcy. W ramach spotkań operacyjnych mogą być omawiane: bieżące tematy operacyjne, informacje dotyczące ostatnich zgłoszeń i Alertów, zaproponowane zmiany w ustaleniach

- operacyjnych. Podczas spotkań operacyjnych nie są podejmowane wiążące decyzje. Decyzje powinny być potwierdzone drogą mailową. Spotkania operacyjne nie obejmują tematów warsztatowych i konsultacyjnych.
- 6) Opiekun techniczny jest dostępny w dni robocze, w godzinach 9:00-17:00.
  - 7) Czas trwania oraz częstotliwość spotkań operacyjnych określono w § 4.
  - 8) W ramach spotkań operacyjnych może być prowadzony przegląd i omówienie procedur, ścieżek eskalacji, konfiguracji monitorowanych systemów oraz parametrów świadczonej Usługi.
  - 9) Wykonawca zastrzega sobie możliwość zawieszenia spotkań na okres do 4 tygodni w ciągu roku z powodu niedostępności dedykowanego opiekuna technicznego.
  - 10) Zamawiający zostanie poinformowany o zawieszeniu spotkań operacyjnych z tygodniowym wyprzedzeniem, a jeżeli zachowanie tego terminu nie będzie możliwe z przyczyn losowych – niezwłocznie po otrzymaniu przez Wykonawcę informacji o niedostępności opiekuna technicznego.
  - 11) Czas z nieodbytych spotkań może zostać wykorzystany w ramach godzin konsultacyjnych.
  - 12) Spotkania operacyjne będą odbywały się on-line.
10. Tuning mechanizmów detekcji monitorowanych systemów bezpieczeństwa
- 1) W ramach możliwości technicznych monitorowanych systemów oraz posiadanych uprawnień Wykonawca będzie implementował zmiany w konfiguracji monitorowanych systemów w celu podniesienia efektywności mechanizmów detekcji oraz ograniczenia ilości fałszywych alarmów.
  - 2) Jeśli Zamawiający nie zapewni Wykonawcy uprawnień, dostępów i zgody na wprowadzanie zmian lub po uzyskaniu zaleceń wynikających z analizy Alertów nie wprowadzi tych zmian samodzielnie, Wykonawca odfiltruje fałszywe alarmy na etapie monitoringu systemów i nie będą one poddawane analizie do czasu potwierdzenia przez Zamawiającego optymalizacji mechanizmów detekcji.
11. Zarządzanie systemami cyberbezpieczeństwa
- 1) Wykonawca zarządza konfiguracją systemów objętych zarządzaniem zgodnie z § 4.
  - 2) Zakres zarządzania obejmuje następujące elementy konfiguracji:
    - a) Użytkownicy i grupy
    - b) Polityki bezpieczeństwa
    - c) Aktualizacje oprogramowania
    - d) Monitoring wydajności
12. Wsparcie techniczne dla systemów cyberbezpieczeństwa
- 1) Wykonawca świadczy Usługi wsparcia technicznego dla systemów objętych wsparciem zgodnie z § 4.

- 2) W ramach wsparcia technicznego Wykonawca będzie podejmował następujące działania:
- a) Przeprowadzanie aktualizacji oprogramowania, zarówno w całości, jak i poszczególnych jego komponentów.
  - b) Zapewni pomoc w rozwiązywaniu problemów technicznych związanych z eksploatacją systemów.
  - c) Zapewni pomoc w kontaktach z producentem systemu.

#### **§ 4 Parametry Usługi**

1. Ustalone kanały komunikacji to:
  - 1) Mail: [.....]
  - 2) Telefon: [telefon dostawcy]
  - 3) Komunikator: Teams
2. Monitorowane systemy bezpieczeństwa:
  - 1) EDR, 400 agentów
  - 2) SIEM, 30 alertów miesięcznie
  - 3) Zgłoszenia za pośrednictwem ustalonych kanałów, do 10 zgłoszeń miesięcznie.
3. Granularność autoryzacji i ścieżek eskalacji jest jednolita dla całej organizacji
4. Czas reakcji dla Alertów i zgłoszeń podejrzenia wystąpienia Incydentów to 120 minut.
5. Okres raportowy to 1 miesiąc.
6. Spotkania operacyjne:
  - 1) Częstotliwość to raz na miesiąc
  - 2) Czas trwania spotkania do 1 godziny.
7. Opiekun techniczny dostępny przez cały okres współpracy.
8. Wsparcie techniczne dla systemów cyberbezpieczeństwa:
  - 1) Systemy objęte wsparciem: EDR, SIEM/XDR
  - 2) Czas reakcji na zgłoszenie problemu technicznego:
    - a) W każdym przypadku niedostępności monitorowanych systemów lub ich nieprawidłowego działania, które negatywnie wpłyną na ich możliwości pod względem gromadzenia danych oraz wykrywania i reakcji na zagrożenia, Wykonawca podejmie działania w celu rozwiązania problemu w czasie do 12 godzin od momentu wykrycia problemu przez Wykonawcę lub zgłoszenia problemu przez Zamawiającego.
    - b) W każdym przypadku nieprawidłowego działania monitorowanych systemów, które negatywnie wpływa na systemy IT Zamawiającego Wykonawca podejmie działania w celu usunięcia problemu w czasie do 6 godzin od wykrycia lub zgłoszenia problemu.
    - c) W każdym przypadku nieprawidłowego działania monitorowanych systemów, które uniemożliwia działanie systemów IT Zamawiającego



Wykonawca podejmie działania w celu usunięcia problemu w czasie do 2 godzin od wykrycia lub zgłoszenia problemu.

9. Zarządzanie systemami cyberbezpieczeństwa
  - 1) Systemy objęte zarządzaniem: EDR, SIEM/XDR
  - 2) Czas reakcji na zgłoszenie w zakresie zarządzania systemami cyberbezpieczeństwa: 48 godzin
10. Dostępność usługi – 99% czasu w każdym miesiącu

### **§ 5 Wykluczenie**

Wykonawca oświadcza, że nie podlega wykluczeniu na podstawie 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 (Dz. U. z 2024 r. poz. 1320 zm.) oraz jest podmiotem gwarantującym bezstronność przy wykonywaniu Umowy.

### **§ 6 Zobowiązania Wykonawcy**

1. Wykonawca zobowiązuje się do wykonywania przedmiotu Umowy z najwyższą starannością z uwzględnieniem zawodowego charakteru prowadzonej działalności, zgodnie z aktualną wiedzą i przyjętymi praktykami w sektorze technologii informatycznych.
2. Wykonawca oświadcza, że zarówno jego pracownicy, współpracownicy i ewentualnie podwykonawcy oraz pracownicy podwykonawców, którymi posługuje się przy wykonaniu Umowy, posiadają odpowiednie kwalifikacje lub zezwolenie odpowiednich organów, jeżeli takie są wymagane przepisami prawa.
3. Dla uniknięcia wątpliwości Strony ustalają, iż wykonanie Umowy przez Wykonawcę może się opóźnić o czas trwania przeszkody wywołanej niewykonaniem przez Zamawiającego lub inne podmioty obowiązków przewidzianych niniejszą Umową lub wynikające z przyczyn leżących poza kontrolą Wykonawcy, jak np. z trwającej pandemii. W tych granicach Wykonawca nie będzie ponosił odpowiedzialności z tytułu niewykonania Umowy w terminie.
4. Wykonawca zobowiązuje się do ewidencjonowania w ramach Systemu Obsługi Zgłoszeń wszelkich działań związanych z wykonywaniem Usług w zakresie, w jakim wymagają tego postanowienia Umowy.
5. Wykonawca zobowiązany jest przestrzegać wszelkich regulaminów, zasad i reguł obowiązujących u Zamawiającego, mających wpływ na świadczenie Usług cyberbezpieczeństwa, pod warunkiem, że Zamawiający prześle je Wykonawcy co najmniej na 7 dni przed rozpoczęciem świadczenia Usług przez Wykonawcę.
6. Wykonawca będzie zobowiązany do niezwłocznego poinformowania ustalonych osób kontaktowych, z zachowaniem ścieżek eskalacji i ustaleń operacyjnych, o wykrytych Incydentach cyberbezpieczeństwa.

7. Wykonawca przez cały okres trwania umowy jest zobowiązany posiadać ubezpieczenie odpowiedzialności cywilnej za szkody wyrządzone w związku z prowadzeniem działalności, na sumę ubezpieczenia nie niższą, niż 3 000 000 zł (trzy miliony złotych). Kopia polisy potwierdzającej zawarcie umowy ubezpieczenia aktualna na dzień zawarcia Umowy stanowi Załącznik nr ..... do Umowy.
8. Wykonawca jest zobowiązany do przedstawienia Zamawiającemu kopii aktualnej polisy ubezpieczenia odpowiedzialności cywilnej na każde jego żądanie, zgłoszone w okresie obowiązywania Umowy, nie później jednak niż w terminie 3 dni roboczych od dnia otrzymania żądania.
9. Wykonawca nie jest uprawniony do dokonywania cesji, przeniesienia bądź obciążenia swoich praw lub obowiązków wynikających z Umowy, bez uprzedniej zgody Zamawiającego, udzielonej na piśmie pod rygorem nieważności.

### **§ 7 Zobowiązania Zamawiającego**

1. Zamawiający jest zobowiązany do udostępnienia Wykonawcy sieci IT, systemów, pomieszczeń, umożliwienie dostępu zdalnego oraz autoryzację działań podejmowanych przez Wykonawcę w ramach świadczonych Usług.
2. Zamawiający zobowiązany jest do wskazania osób uprawnionych do autoryzacji działań Wykonawcy. Osoby te będą wskazane w ramach ustaleń operacyjnych.
3. Osoby wskazane w ramach ustaleń operacyjnych będą upoważnione do autoryzacji Wykonawcy do zastosowania odpowiednich działań mających na celu zwalczenie lub zapobieżenie Incydentowi cyberbezpieczeństwa. W przypadku konieczności podjęcia natychmiastowych działań przez Wykonawcę bez uprzedniej autoryzacji Wykonawca będzie zobowiązany do wskazania podjętych działań oraz ich uzasadnienia.
4. Strony są zobowiązane do współdziałania przy wykonaniu Umowy. W szczególności Zamawiający zobowiązuje się do niezwłocznego ustosunkowania się i rozwiązywania problemów zgłaszanych przez Wykonawcę, nie później jednak niż w terminie 2 dni roboczych od dnia takiego zgłoszenia, chyba że okoliczności sprawy będą wymagały szybszej reakcji, wtedy Zamawiający zobowiązuje się do udzielenia informacji niezwłocznie.
5. Zamawiający oświadcza, iż jest świadomy, że zdolność Wykonawcy do należytego i terminowego zrealizowania przedmiotu Umowy zależy od współpracy obu stron Umowy, a także od dokładności i kompletności wszelkich informacji i danych dostarczonych przez Zamawiającego. Wobec powyższego Zamawiający w szczególności:
  - 1) zapewni dostęp i możliwość wykorzystania wszelkich informacji niezbędnych dla prawidłowej realizacji Umowy, z zachowaniem zasad poufności i bezpieczeństwa obowiązujących u Zamawiającego,

- 2) zapewni, o ile będzie to konieczne, dostęp do elementów infrastruktury i środowiska teleinformatycznego Zamawiającego w zakresie potrzebnym do świadczenia Usług przez Wykonawcę na podstawie Umowy,
- 3) zapewni Wykonawcy kontakt z osobami oddelegowanymi w danym czasie do realizacji Umowy,
- 4) dostarczy Wykonawcy wszelkie niezbędne do należytego wykonania Umowy informacje w terminie nieprzekraczającym 7 dni roboczych od daty, w której zwróci się o nie Wykonawca (z zastrzeżeniem § 7 ust. 4 niniejszej Umowy), chyba że Strony uzgodnią inny termin.

### **§ 8 Zasady prowadzenia ustaleń operacyjnych**

1. W ramach ustaleń operacyjnych zostaną uzgodnione poniższe kwestie:
  - 1) Ścieżki kontaktowe
  - 2) Poziom autoryzacji
2. Wykonawca zobowiązuje się do przekazania taksonomii klasyfikacji Incydentów w procesie obsługi Incydentów Wykonawcy.
3. Ze strony Wykonawcy osobą odpowiedzialną za decyzje operacyjne jest [przedstawiciel Wykonawcy] lub osoba przez niego upoważniona.
4. Ze strony Zamawiającego osobą upoważnioną do podejmowania decyzji w zakresie operacyjnym jest:

### **§ 9 Oprogramowanie dostarczane w ramach umowy**

1. W ramach umowy zostanie dostarczone oprogramowanie klasy EDR.
2. Oprogramowanie klasy EDR zostanie dostarczone w liczbie 400 agentów.
3. Oprogramowanie klasy NDR zostanie zainstalowane na zasobach udostępnionych przez Zamawiającego, zgodnych z wytycznymi przekazanymi przez producenta.

### **§ 10 Warunki korzystania z oprogramowania dostarczonego przez Wykonawcę**

1. Warunki korzystania z oprogramowania EDR  
[Warunki dostarczone przez Wykonawcę]
2. **Warunki korzystania z oprogramowania XDR/SIEM**  
[Warunki dostarczone przez Wykonawcę]

### **§ 11 Wynagrodzenie**

1. Z tytułu realizacji niniejszej Umowy Zamawiający zapłaci Wykonawcy wynagrodzenie całkowite nieprzekraczające kwoty w wysokości netto:  
..... zł (słownie: .....  
złotych..... /100 gr netto), VAT: ..... zł (słownie:  
.....), brutto: .....zł  
(słownie:..... złotych ...../100 gr

brutto), zgodnie z Formularzem cenowym Wykonawcy stanowiącym Załącznik nr ..... do Umowy.

2. Na wynagrodzenie, o którym mowa w ust. 1, składa się wynagrodzenie z tytułu:
  - 1) wdrożenia i uruchomienie Usługi SOC – jednorazowego wynagrodzenia w wysokości netto: ..... zł (słownie: ..... złotych..... /100 gr netto), VAT: ..... zł (słownie: .....), brutto: .....zł (słownie:..... złotych ...../100 gr brutto);
  - 2) świadczenia w danym miesiącu kalendarzowym Usługi SOC – miesięcznego wynagrodzenia w wysokości netto: ..... zł (słownie: ..... złotych..... /100 gr netto), VAT: ..... zł (słownie: .....), brutto: .....zł (słownie:..... złotych ...../100 gr brutto).
3. Wynagrodzenie jest należne z dołu po wykonaniu obowiązków Wykonawcy, o których mowa w ust.2 pkt 1-2.
4. Podstawą do wystawienia faktury z tytułu wynagrodzenia, o którym mowa w ust. 2 pkt 1, jest podpisany przez obie strony protokół odbioru, stwierdzający należyte wykonanie obowiązków Wykonawcy w ramach wdrożenia i uruchomienia Usługi SOC.
5. Podstawą do wystawienia faktury z tytułu wynagrodzenia, o którym mowa w ust. 2 pkt 2, jest oświadczenie Zamawiającego o przyjęciu raportu okresowego, sporządzonego zgodnie z § 3 pkt 8 Umowy, za dany miesiąc kalendarzowy.
6. Zapłata należnego wynagrodzenia nastąpi w terminie do 14 dni od otrzymania faktury na rachunek bankowy Wykonawcy nr .....
7. Za dzień zapłaty faktury uważa się dzień obciążenia rachunku bankowego Zamawiającego.
8. Płatność dokonana będzie na podstawie prawidłowo wystawionej faktury.
9. Wynagrodzenie całkowite określone w ust. 1 zawiera wszelkie koszty związane z realizacją Umowy, w tym przyłączenia do sieci telekomunikacyjnej, wsparcie techniczne, opłaty, podatki i należności wynikające z obowiązujących przepisów prawa.
10. W przypadku gdy rozpoczęcie świadczenia Usługi SOC nie nastąpi pierwszego dnia kalendarzowego miesiąca albo jej zakończenie nie nastąpi ostatniego dnia miesiąca kalendarzowego, miesięczne wynagrodzenie oblicza się proporcjonalnie do ilości dni w miesiącu, w którym Usługa SOC była świadczona przez okres krótszy niż cały miesiąc kalendarzowy.

## **§ 12 Odpowiedzialność**

1. Strony ustalają, iż całkowita odpowiedzialność Wykonawcy z tytułu niewykonania lub nienależytego wykonania Umowy zostaje ograniczona do kwoty:
  - 1) stanowiącej równowartość 200% wartości wynagrodzenia za okres, w którym powstało zdarzenie wywołujące szkodę – w sytuacji, gdy Wykonawca dopuścił się rażącego niedbalstwa,
  - 2) stanowiącej równowartość 100% wartości wynagrodzenia za okres, w którym powstało zdarzenie wywołujące szkodę – w sytuacji innej niż dopuszczenie się przez Wykonawcę rażącego niedbalstwa.
2. Jednocześnie Strony wyłączają odpowiedzialność Wykonawcy z tytułu utraconych korzyści Zamawiającego lub podmiotów trzecich.
3. Strony postanawiają, że Wykonawca będzie ponosił odpowiedzialność wyłącznie za działania swoje lub swoich pracowników, współpracowników, podwykonawców, nie będzie ponosił natomiast jakiegokolwiek odpowiedzialności za niewykonanie lub nienależyte wykonanie Umowy będące skutkiem działania lub zaniechania Zamawiającego lub podmiotów trzecich.
4. Strony wyłączają jakąkolwiek odpowiedzialność spowodowaną działaniem siły wyższej, przez co należy rozumieć zjawiska wyjątkowe, niezależne od Stron takie jak np.:
  - 1) wojnę, w tym: wojnę domową, zamieszki, rozruchy i akty sabotażu,
  - 2) katastrofę naturalną, przykładowo silną burzę, huragan, trzęsienie ziemi, powódź, zniszczenie przez piorun,
  - 3) wybuch, pożar, zniszczenie maszyn lub wszelkiego rodzaju instalacji,
  - 4) bojkot, strajk, lock-outy wszelkiego rodzaju, strajk „włoski”, okupowanie pomieszczeń, pandemie itp.
5. Strony uwzględniają, że biorąc pod uwagę charakter świadczonych Usług, niezwykle trudne jest zagwarantowanie lub zapobieżenie wszelkim zagrożeniom bezpieczeństwa, naruszeniom danych lub innym towarzyszącym stratom, związanymi z Incydentami cyberbezpieczeństwa. Umowa nie jest umową rezultatu, a umową starannego działania.
6. Wykonawca ponosi na zasadach ogólnych odpowiedzialność obejmującą utratę, uszkodzenie lub zniszczenie plików programowych Zamawiającego, urządzeń, danych, sprzętu komputerowego lub oprogramowania komputerowego, wynikającego z Usług lub oprogramowania dostarczonego na podstawie Umowy.
7. Wykonawca będzie odpowiedzialny za dane osobowe, rozumiane jako informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, przekazane przez Zamawiającego w wykonaniu niniejszej Umowy, w zakresie i na podstawie zawartej pomiędzy Stronami umowy powierzenia przetwarzania danych osobowych, której wzór stanowi Załącznik nr 2.
8. Wykonawca przed rozpoczęciem świadczenia Usług i przed podpisaniem umowy powierzenia przetwarzania danych osobowych zobowiązany jest umożliwić



przeprowadzenie audytu w zakresie wypełnionej i załączonej do Oferty ankiety bezpieczeństwa. Ankieta stanowi załącznik nr ... do Umowy.

9. Ankieta stanowi element weryfikacji podmiotu przetwarzającego przed zawarciem umowy powierzenia przetwarzania danych osobowych oraz określonego w umowie powierzenia przetwarzania danych osobowych obowiązku wynikającego z art. 28 ust. 3 lit. h Rozporządzenia 2016/679.
10. Czynności podejmowane w trakcie audytu nie są postępowaniem, o którym mowa w art. 58 ust. 1 lit. b Rozporządzenia 2016/679, co nie wyłącza możliwości wszczęcia przez Prezesa Urzędu Ochrony Danych Osobowych z urzędu postępowania w przypadku powzięcia informacji o naruszeniu Rozporządzenia 2016/679.

### **§ 13 Odstąpienie od umowy**

1. Zamawiający może odstąpić od Umowy w przypadkach określonych w przepisach obowiązującego prawa, w szczególności Kodeksu cywilnego.
2. Zamawiający może odstąpić od umowy z przyczyn leżących po stronie Wykonawcy, gdy:
  - 1) Wykonawca opóźnia się w spełnieniu przedmiotu umowy powyżej 7 dni roboczych;
  - 2) Wykonawca nienależycie wykonuje umowę, w szczególności nie stosuje się do uwag Zamawiającego lub narusza inne postanowienia Umowy i w przypadku, gdy po upływie 7 dni od wezwania przez Zamawiającego do zaniechania przez Wykonawcę naruszeń postanowień umowy i usunięcia ewentualnych skutków naruszeń, Wykonawca nie zastosuje się do wezwania.
  - 3) Wykonawca nie wypełni ankiety, o której mowa w § 12 ust. 8 lub nie wdroży odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia 2016/679 i chroniło prawa osób, których dane dotyczą, co obejmuje również negatywny wynik audytu.
3. Zamawiający może odstąpić od Umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu. W tym przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu należytego wykonania części umowy.
4. Prawo odstąpienia Zamawiający może wykonać w terminie 30 dni od powzięcia wiadomości o okolicznościach, o których mowa w niniejszym paragrafie.
5. Odstąpienie od umowy następuje w formie pisemnej pod rygorem nieważności i wymaga uzasadnienia.
6. W przypadku odstąpienia od umowy Zamawiający nie traci uprawnień do naliczania należnych z tytułu odstąpienia od Umowy kar umownych.

### **§ 14 Termin i warunki realizacji umowy**

1. Wykonawca przygotowuje plan wdrożenia Usługi, który przedłoży Zamawiającemu w ciągu 7 dni od podpisania niniejszej umowy. Zamawiający może zgłosić zastrzeżenia w ciągu 7 dni. Plan będzie zawierał informacje o działaniach koniecznych w celu wdrożenia Usługi.
2. Termin rozpoczęcia usługi SOC wynosi do 30 dni od dnia zawarcia umowy. W przypadku nienależytego wykonania obowiązków w powyższym terminie Zamawiającemu przysługuje kara umowna, o której mowa w § 15 ust.3.
3. Usługa SOC będzie świadczona przez okres 12 miesięcy od dnia podpisania przez Zamawiającego protokołu odbioru bez uwag oraz zastrzeżeń, potwierdzającego zakończenie wdrożenia usługi SOC.
4. Z odbioru wdrożenia usługi SOC zostanie sporządzony i podpisany protokół odbioru przez osobę wyznaczoną przez Zamawiającego. Protokół odbioru powinien zawierać w szczególności:
  - 1) datę i miejsce odbioru,
  - 2) ocenę prawidłowości wykonania czynności oraz zgodności wykonania z postanowieniami Umowy oraz OPZ,
  - 3) oświadczenie osoby powołanej do odbioru ze strony Zamawiającego o istnieniu bądź braku wad,
  - 4) w przypadku stwierdzenia wad lub nieprawidłowości – zobowiązanie Wykonawcy do ich usunięcia w terminie wskazanym przez Zamawiającego. Wzór Protokołu Odbioru stanowi Załącznik nr .... do Umowy.
5. Umowa może zostać wypowiedziana przez Zamawiającego jedynie z ważnego powodu, za który Strony będą uznawać wyłącznie rażące naruszenie przez Wykonawcę obowiązków wynikających z niniejszej Umowy. W takiej sytuacji wypowiedzenie może zostać dokonane z zachowaniem miesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca kalendarzowego, pod warunkiem, że Zamawiający wezwie Wykonawcę do zaprzestania naruszeń Umowy w odpowiednim terminie, nie krótszym niż 30 dni i po bezskutecznym upływie tego terminu.
6. Wykonawca może wypowiedzieć Umowę w każdym czasie, bez zachowania okresu wypowiedzenia, jeżeli Zamawiający nie opłaci (w jakiegokolwiek części) co najmniej dwóch faktur, obejmujących wynagrodzenie Wykonawcy wynikające z niniejszej Umowy – pod warunkiem uprzedniego wyznaczenia przez Wykonawcę dodatkowego terminu, nie krótszego niż 30 dni i po bezskutecznym upływie tego terminu na uregulowanie całego zadłużenia.

### **§ 15 Kary umowne**

1. W przypadku odstąpienia od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% kwoty łącznego wynagrodzenia brutto, o której mowa w § 11 ust.

- 1, przy czym w przypadku odstąpienia od części Umowy, podstawą naliczenia kary umownej jest wartość umowy brutto w części objętej odstąpieniem.
2. W przypadku odstąpienia od Umowy przez Wykonawcę z przyczyn leżących po jego stronie, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% kwoty łącznego wynagrodzenia brutto, o której mowa w § 11 ust. 1 przy czym w przypadku odstąpienia od części Umowy, podstawą naliczenia kary umownej jest wartość umowy brutto w części objętej odstąpieniem.
3. Wykonawca zapłaci Zamawiającemu karę umowną w razie zwłoki w wykonaniu czynności uruchomienia usługi SOC w terminie, o którym mowa w § 14 ust. 2 – w wysokości 0,1% wynagrodzenia brutto określonego w § 11 ust. 1, za każdy dzień zwłoki.
4. Za każdą rozpoczętą godzinę zwłoki w stosunku do maksymalnego czasu określonego w § 4 Umowy, Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 200 zł.
5. Łączna suma naliczonych kar umownych nie przekroczy 30% kwoty łącznego wynagrodzenia, o której mowa w § 11 ust. 1.
6. Wykonawca nie będzie obciążany karami umownymi jeśli do niewykonania Umowy doszło z powodu okoliczności, za które odpowiedzialność ponosi Zamawiający.
7. Kary umowne, o których mowa w niniejszym paragrafie, są wymagalne w terminie 7 dni od dnia doręczenia Wykonawcy oświadczenia o ich nałożeniu. Kary umowne będą w pierwszej kolejności potrącane z wynagrodzenia należnego Wykonawcy, na co Wykonawca wyraża zgodę i do czego upoważnia Zamawiającego bez potrzeby uzyskiwania pisemnego potwierdzenia.
8. Kary umowne przewidziane w niniejszym paragrafie obowiązują niezależnie od siebie, z tym zastrzeżeniem, że w przypadku odstąpienia od umowy, możliwe jest naliczenie wyłącznie kary przewidzianej na wypadek odstąpienia od umowy, z tym, że w przypadku odstąpienia od części umowy zastrzeżenie to dotyczy tylko części umowy objętej odstąpieniem.
9. Odstąpienie od Umowy przez którąkolwiek ze Stron, nie powoduje utraty prawa przez Zamawiającego do kar umownych należnych na podstawie umowy.
10. Zapłata przez Wykonawcę kar umownych z tytułu niewykonania lub nienależytego wykonania Umowy, nie wyłącza prawa Zamawiającego do dochodzenia odszkodowania przewyższającego ustalone powyżej kary umowne na zasadach ogólnych.

### **§ 16 Poufność**

1. Strony zobowiązują się do zachowania w poufności wszelkich otrzymanych od drugiej Strony informacji, w tym technicznych, technologicznych, ekonomicznych, finansowych, handlowych, prawnych, organizacyjnych i innych otrzymanych lub powierzonych bądź pozyskanych do przetwarzania w związku z zawarciem lub realizacją Umowy, niezależnie od formy ich utrwalenia lub przekazania,

oznaczonych jako „Informacje Poufne”, a które nie zostały podane do publicznej wiadomości. W celu wyjaśnienia wszelkich ewentualnych wątpliwości Strony postanawiają, że Informacje Poufne obejmują również jedną poszczególną informację lub jej część.

2. W szczególności Strony zobowiązują się:
  - 1) utrzymać w tajemnicy i chronić przed nieautoryzowanym użyciem Informacje Poufne otrzymane od drugiej Strony, bez względu na nośnik Informacji Poufnych, jak i sposób ich ujawnienia,
  - 2) wykorzystywać Informacje Poufne tylko w celu realizacji Umowy i ujawniać Informacje Poufne tylko swoim pracownikom lub współpracownikom bezpośrednio zaangażowanym w realizację Umowy,
  - 3) przedsięwziąć wszelkie niezbędne środki w celu zapewnienia, iż żadna osoba, która otrzyma Informacje Poufne, nie ujawni ich osobom trzecim bez uzyskania pisemnej zgody Strony,
  - 4) przestrzegać instrukcji i poleceń, które wynikają z wewnętrznych regulacji każdej ze Stron, a z którymi została ona właściwie zapoznana,
  - 5) stosować odpowiednie zabezpieczenia wszelkich nośników i dokumentów, zawierających Informacje Poufne,
  - 6) do nieujawniania i ochrony Informacji Poufnych zarówno w czasie trwania Umowy, jak i przez 10 lat po jej zakończeniu (po upływie tego okresu, zobowiązanie przekształca się w zobowiązanie na czas nieokreślony, z 3-letnim okresem wypowiedzenia),
  - 7) do nieprzetrzymania Informacji Poufnych dłużej niż jest to konieczne do realizacji Umowy, jak również do zwrócenia pochodzących od drugiej Strony Informacji Poufnych wraz z wszystkimi kopiami, zrobionymi na potrzeby Projektu natychmiast po zrealizowaniu Projektu lub do zniszczenia Informacji Poufnych wraz z wszystkimi kopiami po otrzymaniu od Strony zgody, według ustalonej procedury i metody niszczenia,
  - 8) do natychmiastowego powiadomienia drugiej Strony o nieautoryzowanym użyciu lub ujawnieniu Informacji Poufnych, jak i do współpracy w celu wprowadzenia środków zaradczych zapobiegających nieautoryzowanemu użyciu i ujawnieniu informacji poufnych.
3. Postanowienia ust. 1 i 2 nie będą miały zastosowania do Informacji Poufnych, które:
  - 1) zostały zgodnie z prawem przekazane i lub ujawnione przez osobę trzecią, bez naruszania jakichkolwiek zobowiązań o ich nieujawnianiu w stosunku do Stron,
  - 2) zostały ujawnione na podstawie odpowiedniego przepisu prawa, wyroku sądowego lub decyzji administracyjnej.
4. Strona, która przez swoje działanie lub zaniechanie dopuszcza się bezprawnego ujawnienia Informacji Poufnych, zobowiązana będzie do zapłaty kary umownej w

wysokości 50.000,00 zł (słownie: pięćdziesięciu tysięcy złotych), w terminie 14 (czternastu) dni od doręczenia jej wezwania, na rachunek wskazany w tym wezwaniu. Strona odpowiada za ujawnienie Informacji Poufnych przez swoich pracowników lub współpracowników jak za swoje własne działania lub zaniechania.

### **§ 17 Zmiany Umowy**

1. Niedopuszczalne są istotne zmiany Umowy, o których mowa w art. 454 ustawy Prawo zamówień publicznych.
2. Zamawiający przewiduje możliwość zmian postanowień Umowy w przypadkach, gdy:
  - 1) nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację Przedmiotu Umowy, chyba że zmiana taka znana była w chwili składania oferty;
  - 2) niezbędna jest zmiana sposobu wykonania zobowiązania, z wyjątkiem sytuacji, gdy zmiana ta ingeruje w treść oferty lub jest istotna, lub o ile zmiana taka jest konieczna w celu prawidłowego wykonania Przedmiotu Umowy;
  - 3) niezbędna jest zmiana terminu realizacji Umowy w przypadku zaistnienia okoliczności lub zdarzeń uniemożliwiających realizację Umowy w wyznaczonym terminie, na które Strony nie miały wpływu.
3. Zmiana Umowy wymaga aneksu w formie pisemnej lub postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, pod rygorem nieważności.
4. Zmiany Umowy nie stanowią zmian nazw/określeń Stron, siedziby Stron, numerów rachunków bankowych Stron, jak również osób odpowiedzialnych za realizację przedmiotu Umowy ze strony Wykonawcy oraz przedstawicieli Zamawiającego.

### **§ 18 Ochrona danych osobowych, klauzule informacyjne**

W związku z udostępnianiem sobie wzajemnie przez Strony (administratorów danych) danych osobowych, Strony zamieszczają postanowienia określające jego zakres oraz wymagane informacje:

- 1) dane osobowe osób reprezentujących każdą ze Stron wymienionych w części wstępnej Umowy oraz osób wyznaczonych do kontaktów i dokonywania bieżących uzgodnień oraz nadzoru nad realizacją umowy, a ponadto upoważnionych przez Wykonawcę do wystawienia faktury udostępniane będą drugiej Stronie i będą przetwarzane w celu realizacji Umowy (podstawa przetwarzania danych osobowych – art. 6 ust. 1 pkt b, pkt c, pkt e Rozporządzenia 2016/679).
- 2) każda ze Stron oświadcza, że jej pracownicy wymienieni wyżej w pkt. 1 w zakresie swoich obowiązków zostaną zaznajomieni z niniejszą Umową, w tym z zapisami zawartymi poniżej w pkt. 3–5.



- 3) każda z osób wymienionych powyżej, w pkt. 1 ma prawo żądania dostępu do swoich danych osobowych, ich sprostowania oraz prawo wniesienia sprzeciwu wobec przetwarzania danych osobowych, a także prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w wypadku uznania, że administrator naruszył przepisy o ochronie danych osobowych. Dane będą ujawniane uprawnionym pracownikom Stron oraz podmiotom i ich pracownikom świadczącym usługi prawne, finansowe, księgowe i informatyczne.
- 4) Wykonawca podaje, że dane te będzie przetwarzał w okresie koniecznym do realizacji i rozliczenia Umowy z uwzględnieniem okresu przedawnienia oraz przepisów podatkowych oraz, iż powoła osobę odpowiedzialną (np. inspektora ochrony danych osobowych lub inną) z którą można będzie skontaktować się poprzez [.....].
- 5) Zamawiający podaje, że dane te będzie przetwarzał w okresie koniecznym do realizacji i rozliczenia Umowy, z uwzględnieniem okresu przedawnienia oraz przepisów podatkowych, oraz iż powołał inspektora ochrony danych, z którym można się skontaktować poprzez adres email: [iod@uodo.gov.pl](mailto:iod@uodo.gov.pl) lub pod numerem telefonu [.....].

### **§ 19 Postanowienia końcowe**

1. Zmiana Umowy wymaga aneksu w formie pisemnej lub postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, pod rygorem nieważności.
2. W razie uznania któregośkolwiek postanowienia niniejszej Umowy za nieważne lub bezskuteczne, Umowa pozostaje w mocy w pozostałym zakresie. Strony zobowiązują się do zastąpienia nieważnego lub bezskutecznego postanowienia postanowieniem, które najlepiej odzwierciedlać będzie zgodną wolę Stron i ich słuszne interesy.
3. Wykonawca nie może przenieść na osobę trzecią praw i obowiązków wynikających z Umowy, w całości lub w części.
4. Umowa podlega prawu polskiemu i zgodnie z nim powinna być interpretowana.
5. Strony komunikują się w języku polskim, co obejmuje w szczególności świadczenie Usług.
6. Strony Umowy podejmą w dobrej wierze wysiłek w celu rozwiązania wszelkich sporów powstałych pomiędzy Stronami, które wynikły w związku z realizacją Umowy lub jej interpretacją. O ile rozwiązanie sporu nie powiedzie się, zostanie on poddany pod rozstrzygnięcie sądu powszechnego właściwego miejscowo dla siedziby Zamawiającego.
7. Umowa zostaje zawarta z dniem jej podpisania przez obie strony, w dacie złożenia podpisu przez ostatnią z nich.

W imieniu Wykonawcy:

---

W imieniu Zamawiającego:

---

Załącznik nr ....  
do umowy nr UODO/2026/.../...  
z dnia ..... 2026 r.

Warszawa dn. ....

### Protokół odbioru

Niniejszym stwierdzamy, że przedmiot umowy pt. „Wdrożenie i świadczenie usługi SOC (Security Operation Center)” zgodnie z umową nr..... z dnia ..... w części dotyczącej wdrożenia i uruchomienie usługi SOC (Security Operation Center) u Zamawiającego został/nie został wykonany zgodnie z umową w terminie tj. do dnia ...../niezgodnie z umową po terminie tj. do dnia .....

Przedmiot umowy pt. „Wdrożenie i świadczenie usługi SOC (Security Operation Center)” we wskazanej wyżej części przyjęto bez zastrzeżeń/ z następującymi zastrzeżeniami\*:

.....  
.....  
.....  
.....  
.....

W przypadku konieczności szerszego wyjaśnienia powstałych zastrzeżeń dołączona zostanie odrębna karta (stanowiąca integralną część protokołu odbioru)

Naliczono kary

1. TAK zgodnie z § ..... ww. umowy w wysokości ..... (słownie: .....)
2. NIE\*

Przedmiot umowy w ramach umowy nr..... z dnia ..... „Wdrożenie usługi SOC” będzie współfinansowany w ramach grantu otrzymanego przez Zamawiającego w ramach przedsięwzięcia Inwestycja

C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd Krajowego Planu Odbudowy i Zwiększania Odporności.

Sporządził i sprawdził pod kątem merytorycznym .....

Podpis Zamawiającego

Podpis Wykonawcy

.....  
.....

\*niepotrzebne skreślić

## Załącznik nr 3 do SWZ

Wykonawca:

.....  
.....  
.....

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP, KRS/CEiDG)

reprezentowany przez:

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

## Załącznik nr 3

Ankieta stanowi realizację określonego w umowie powierzenia przetwarzania danych osobowych obowiązku wynikającego z art. 28 ust. 3 lit. h Rozporządzenia 2016/679.

Czynności podejmowane w trakcie audytu nie są postępowaniem, o którym mowa w art. 58 ust. 1 lit. b Rozporządzenia 2016/679, co nie wyłącza możliwości wszczęcia z urzędu postępowania w przypadku powzięcia informacji o naruszeniu Rozporządzenia 2016/679.



**Zakres weryfikacji zgodności przetwarzania Danych Osobowych z postanowieniami Umowy o powierzeniu przetwarzania danych osobowych**

**Uwaga: dane zawarte w ankiecie mają charakter poufny. Przesyłanie wypełnionych ankiet wyłącznie w postaci zabezpieczonej hasłem. Hasła należy przysyłać wykorzystując inne kanały komunikacji niż użyte do przysyłania samej ankiety.**

**Dane podmiotu przetwarzającego**

Firma (pełna nazwa podmiotu, bez znaków dodatkowych typu „”):	
NIP	
REGON	
KRS	
Adres siedziby	
Adres świadczenia usług dla administratora (jeżeli inny niż powyżej)	
Dane kontaktowe (dane osoby wskazanej do kontaktu z administratorem)	

**Pytania wstępne**

Lp.	Pytanie	Tak/Nie	Uwagi/komentarze
1.	Czy podmiot przetwarzający przyjął zatwierdzony kodeks postępowania (art. 40 Rozporządzenia 2016/679)?		
2.	Czy podmiot przetwarzający jest certyfikowany zgodnie z zatwierdzonym mechanizmem certyfikacji (art. 42 Rozporządzenia 2016/679)?		
3.	Czy podmiot przetwarzający jest certyfikowany innymi certyfikatami jakości lub w myśl norm ISO? Jeżeli tak, proszę w uwagach podać jakimi i na jaki okres (do kiedy) obowiązuje certyfikacja		

**Organizacja wewnętrzna – osoby funkcyjne**

Lp.	Pytanie	Tak/Nie	Uwagi/komentarze
4.	Czy podmiot przetwarzający powołał lub wyznaczył Inspektora Ochrony Danych (IOD)?		
	Jeżeli nie – proszę przejść do pytania 10.		
5.	Czy IOD został zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych?		
6.	Czy dane IOD zostały opublikowane na stronie podmiotu przetwarzającego?		
7.	Czy IOD posiada zastępcę?		
	Jeżeli nie – proszę przejść do pytania 10.		
8.	Czy zastępca IOD został zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych?		
9.	Czy dane zastępcy IOD zostały opublikowane na stronie podmiotu przetwarzającego?		
10.	Czy podmiot przetwarzający powołał lub wyznaczył inną osobę, która zajmuje się monitorowaniem przestrzegania przepisów dotyczących przetwarzania i ochrony danych osobowych u podmiotu przetwarzającego?		
11.	Czy podmiot przetwarzający powołał lub wyznaczył Administratora Systemów Informatycznych (ASI) lub inną osobę, która z technicznego punktu widzenia odpowiada za infrastrukturę i sieć w podmiocie przetwarzającym?		

Urząd Ochrony Danych Osobowych  
ul. Stanisława Moniuszki 1A  
00-014 Warszawa

[www.uodo.gov.pl](http://www.uodo.gov.pl)

Zabezpieczenia organizacyjne – dokumentacja wewnętrzna			
Lp.	Pytanie	Tak/Nie	Uwagi/komentarze
12.	Czy podmiot przetwarzający przeprowadził analizę ryzyka w zakresie podatności i zagrożeń związanych z wykorzystywanymi przez siebie zasobami (aktywami), które są wykorzystywane przy przetwarzaniu powierzonych danych osobowych? Jeżeli tak, w uwagach proszę wskazać datę ostatniej analizy ryzyka.		
13.	Czy podmiot przetwarzający przeprowadził analizę ryzyka w zakresie zagrożeń dla praw i wolności podmiotów danych w związku z powierzanymi czynnościami oraz ocenę skutków dla ochrony danych? Jeżeli tak, w uwagach proszę wskazać datę przeprowadzenia ostatniej analizy ryzyka.		
14.	Czy podmiot przetwarzający posiada i wdrożył polityki ochrony danych osobowych, o których mowa w art. 24 ust. 2 Rozporządzenia 2016/679? Jeżeli tak, w uwagach proszę wskazać jakie.		
15.	Czy podmiot przetwarzający posiada i wdrożył (w ramach innych polityk/procedur lub jako indywidualny dokument) procedury postępowania w przypadku incydentów bezpieczeństwa i naruszeń ochrony danych osobowych?		
16.	Czy podmiot przetwarzający posiada i wdrożył plany ciągłości działania?		
17.	Czy istnieją inne formalne procedury wspierające zgodne z prawem i bezpieczne przetwarzanie danych osobowych u podmiotu przetwarzającego? Czy procedury te zostały wdrożone i mają zastosowanie do przetwarzania powierzonych danych osobowych?		
18.	Czy podmiot przetwarzający prowadzi rejestry, o których mowa w Rozporządzeniu 2016/679? (w tym: rejestr czynności przetwarzania, rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora)		
Zabezpieczenia organizacyjno-techniczne – upoważnienia i uprawnienia			
Lp.	Pytanie	Tak/Nie	Uwagi/komentarze
19.	Czy osobom, które przetwarzają powierzone dane osobowe, nadano upoważnienia do przetwarzania danych?		
20.	Czy osoby, które przetwarzają powierzone dane osobowe, zostały przeszkolone z zakresu bezpieczeństwa informacji i danych osobowych?		
21.	Czy podmiot przetwarzający opracował i realizuje program szkoleń cyklicznych lub uzupełniających dla osób upoważnionych?		
22.	Czy osoby, które przetwarzają powierzone dane osobowe, zostały zobowiązane do zachowania poufności tych danych, sposobów ich przetwarzania i zabezpieczenia?		
23.	Czy podmiot przetwarzający prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych?		
Zabezpieczenia organizacyjne – współpraca z podwykonawcami			
Lp.	Pytanie	Tak/Nie	Uwagi/komentarze
24.	Czy podmiot przetwarzający korzysta z usług podwykonawców, którym powierza do przetwarzania dane osobowe? <i>Jeżeli nie – proszę przejść do pytania 28.</i>		
25.	Czy podmiot przetwarzający prowadzi rejestr/ewidencję podmiotów przetwarzających/dalszych podmiotów przetwarzających lub inny adekwatny dokument?		
26.	Czy podmiot przetwarzający przy wyborze swojego podwykonawcy przeprowadzania działania preaudytowe, weryfikujące, czy podwykonawca spełnia wystarczające gwarancje wdrożenia odpowiednich środków zabezpieczających, by przetwarzanie spełniało wymogi Rozporządzenia 2016/679 i chroniło podmioty danych?		
27.	Czy podmiot przetwarzający przeprowadza doraźne lub bieżące audyty/kontrole swoich podwykonawców?		
Zabezpieczenia organizacyjne – zabezpieczenia fizyczne obszaru przetwarzania danych osobowych			
Lp.	Pytanie	Tak/Nie	Uwagi/komentarze

28.	Czy obszar fizyczny, gdzie są przetwarzane dane osobowe, został zabezpieczony przed dostępem osób nieuprawnionych? Jeżeli tak, w uwagach proszę opisać, jakie zabezpieczenia fizyczne zastosowano.		
29.	Czy podmiot przetwarzający wprowadził regulacje ograniczające możliwość przebywania osób postronnych w obszarze, gdzie są przetwarzane dane osobowe?		
30.	Czy podmiot przetwarzający korzysta z usług zewnętrznych firm sprzętających/ochroniarskich lub innych, które dla realizacji swoich obowiązków muszą mieć zapewniony dostęp do obszaru przetwarzania danych osobowych? Jeżeli tak, czy dostęp tych osób do obszaru przetwarzania danych osobowych został uregulowany w sposób gwarantujący poufność przetwarzanych danych?		
31.	Czy podmiot przetwarzający opracował i posiada politykę kluczy?		
32.	Czy obszar fizyczny, gdzie są przetwarzane dane osobowe, został objęty nadzorem monitoringu wizyjnego?		
33.	Czy podmiot przetwarzający opracował i wdrożył regulacje dotyczące prowadzenia monitoringu wizyjnego w obiekcie?		
34.	Czy obszar objęty monitoringiem został oznaczony za pomocą odpowiedniej ikonografiki, a osobom wchodzącym na teren objęty monitoringiem są przekazywane informacje o przetwarzaniu ich danych osobowych?		
35.	Czy obszar fizyczny, gdzie są przetwarzane dane osobowe, został objęty systemem alarmowym?		
36.	Czy obszar fizyczny, gdzie są przetwarzane dane osobowe, został wyposażony w systemy przeciwpożarowe?		
<b>Zabezpieczenia organizacyjne – przechowywanie i niszczenie nośników danych</b>			
<b>Lp.</b>	<b>Pytanie</b>	<b>Tak/Nie</b>	<b>Uwagi/komentarze</b>
37.	Czy podmiot przetwarzający opracował i wdrożył zasady bezpiecznego przechowywania nośników danych osobowych (w tym nośników papierowych/tradycyjnych i nośników pamięci elektronicznych)?		
38.	Czy podmiot przetwarzający opracował i wdrożył politykę czystego biurka lub czystego ekranu?		
39.	Czy podmiot przetwarzający opracował i wdrożył zasady wykonywania, przechowywania, weryfikacji i niszczenia kopii zapasowych nośników danych (w tym nośników papierowych/tradycyjnych i nośników pamięci elektronicznych)?		
40.	Czy podmiot przetwarzający opracował i wdrożył zasady niszczenia nośników danych osobowych (w tym nośników papierowych/tradycyjnych i nośników pamięci elektronicznych)?		
41.	Czy podmiot przetwarzający korzysta z usług wyspecjalizowanych podmiotów zajmujących się niszczeniem nośników zawierających dane poufne?		
<b>Zabezpieczenia organizacyjno-techniczne – praca zdalna</b>			
<b>Lp.</b>	<b>Pytanie</b>	<b>Tak/Nie</b>	<b>Uwagi/komentarze</b>
42.	Czy podmiot przetwarzający dopuszcza pracowników do pracy zdalnej?		
	Jeżeli nie – proszę przejść do pytania 44.		
43.	Czy podmiot przetwarzający opracował i wdrożył środki zabezpieczające (organizacyjne, organizacyjno-techniczne, techniczne) umożliwiające prowadzenie bezpiecznej pracy zdalnej		
<b>Zabezpieczenia organizacyjno-techniczne – korzystanie ze sprzętu i urządzeń</b>			
<b>Lp.</b>	<b>Pytanie</b>	<b>Tak/Nie</b>	<b>Uwagi/komentarze</b>
44.	Czy podmiot przetwarzający opracował i wdrożył zasady korzystania ze sprzętu służbowego udostępnianego pracownikom?		
45.	Czy podmiot przetwarzający zezwala na wynoszenie sprzętu służbowego lub urządzeń przydzielanych pracownikom poza obszar przetwarzania danych osobowych?		
	Jeżeli nie – proszę przejść do pytania 47.		
46.	Czy podmiot przetwarzający opracował i wdrożył zasady zabezpieczenia sprzętu służbowego lub urządzeń przydzielanych pracownikom wynoszonych poza obszar przetwarzania danych osobowych, w szczególności, czy zostały wdrożone zasady szyfrowania dysków pamięci takiego sprzętu/urządzeń?		

47.	Czy podmiot przetwarzający zezwala na korzystanie ze służbowego sprzętu i urządzeń przydzielanych pracownikom do celów prywatnych?		
48.	Czy podmiot przetwarzający prowadzi ewidencję wydanego sprzętu służbowego i urządzeń przydzielanych pracownikom?		
49.	Czy podmiot przetwarzający zezwala na korzystanie z pendrive'ów i urządzeń/dysków pamięci zewnętrznej przez pracowników?		
	<i>Jeżeli nie – proszę przejść do pytania 51.</i>		
50.	Czy podmiot przetwarzający wdrożył zasady dotyczące szyfrowania pendrive'ów i urządzeń/dysków pamięci zewnętrznej wykorzystywanych przez pracowników?		
51.	Czy pracownicy mają możliwość instalacji własnego oprogramowania na urządzeniach/sprzęcie oddanym im w użytkowanie przez podmiot przetwarzający?		
52.	Czy pracownicy mają możliwość korzystania z oprogramowania w wersji portable (bez instalacji) na urządzeniach/sprzęcie oddanym im w użytkowanie przez podmiot przetwarzający?		
53.	Czy podmiot przetwarzający rejestruje aktywność użytkowników sprzętu służbowego/urządzeń służbowych z wykorzystaniem tzw. innych form monitoringu?		
	<i>Jeżeli nie – proszę przejść do pytania 54.</i>		
54.	Czy pracownicy podmiotu przetwarzającego zostali poinformowani o prowadzeniu tzw. innych form monitoringu wobec nich?		
<b>Zabezpieczenia organizacyjno-techniczne – sprzęt</b>			
<b>Lp.</b>	<b>Pytanie</b>	<b>Tak/Nie</b>	<b>Uwagi/komentarze</b>
55.	Czy podmiot przetwarzający opracował i wdrożył zasady konserwacji sprzętu i urządzeń wykorzystywanych do przetwarzania danych osobowych?		
56.	Czy podmiot przetwarzający opracował i wdrożył zasady napraw w przypadku awarii lub uszkodzenia sprzętu i urządzeń wykorzystywanych do przetwarzania danych osobowych?		
57.	Czy do realizacji powyższych czynności podmiot przetwarzający korzysta z usług innych wyspecjalizowanych podmiotów?		
58.	Czy podmiot przetwarzający posiada pomieszczenie specjalne o statusie serwerowni?		
59.	Czy podmiot przetwarzający korzysta z pomieszczenia serwerowni wynajmowanego na zasadzie kolokacji od innego dostawcy?		
	<i>Jeżeli nie – proszę przejść do pytania 62.</i>		
60.	Czy podmiot przetwarzający korzysta z serwerowni i serwera należącego do dostawcy zewnętrznego (właściciela powierzchni serwerowej i maszyny fizycznej)?		
	<i>Jeżeli nie – proszę przejść do pytania 62.</i>		
61.	Czy z dostawcami usług wskazanymi w pytaniu 59 lub 60 zawarto umowy regulujące kwestie zabezpieczenia pomieszczenia serwerowni/wynajmowanej powierzchni i maszyny fizycznej?		
62.	Czy podmiot przetwarzający opracował i wdrożył zasady zabezpieczenia pomieszczenia serwerowni, obejmujące zabezpieczenia środowiska serwerowni, dostępu, przeciwdziałające awarii zasilania, dostaw łącza Internet itp.?		
63.	Czy maszyna fizyczna (serwer) został zabezpieczony przed nieuprawnioną ingerencją lub dostępem, np. z wykorzystaniem firewall?		
	<i>Jeżeli nie – proszę przejść do pytania 65.</i>		
64.	Czy firewall stosowany dla zabezpieczenia serwera został indywidualnie skonfigurowany (nie są wykorzystywane ustawienia defaultowe)?		
<b>Zabezpieczenia techniczne – oprogramowanie</b>			
<b>Lp.</b>	<b>Pytanie</b>	<b>Tak/Nie</b>	<b>Uwagi/komentarze</b>
65.	Czy system operacyjny wykorzystywany na sprzęcie/urządzeniach podmiotu przetwarzającego jest regularnie aktualizowany zgodnie z zaleceniami dostawcy systemu?		

66.	Czy podmiot przetwarzający korzysta wyłącznie z oprogramowania, dla którego posiada odpowiednie licencje, uprawniające do wykorzystania oprogramowania w celach komercyjnych?		
67.	Czy na stacjach roboczych zostało zainstalowane oprogramowanie antywirusowe?		
	<i>Jeżeli nie – proszę przejść do pytania 70.</i>		
68.	Czy wdrożono zasady dotyczące aktualizacji oprogramowania antywirusowego i baz sygnatur wirusów?		
69.	Czy wdrożono mechanizmy pozwalające na bieżącą lub doraźną weryfikację aktualności oprogramowania antywirusowego i baz sygnatur wirusów?		
70.	Czy podmiot przetwarzający korzysta z oprogramowania antyspamowego (jako modułu wbudowanego w oprogramowanie antywirusowe lub jako oddzielnego oprogramowania)?		
71.	Czy podmiot przetwarzający korzysta z oprogramowania pozwalającego na bezpieczne przechowywanie kluczy logowania do różnych systemów przez użytkowników?		
<b>Zabezpieczenia techniczne – sieć</b>			
<b>Lp.</b>	<b>Pytanie</b>	<b>Tak/Nie</b>	<b>Uwagi/komentarze</b>
72.	Czy podmiot przetwarzający korzysta z zapory sieciowej/firewalla dla zabezpieczenia sieci wewnętrznej?		
	<i>Jeżeli nie – proszę przejść do pytania 74.</i>		
73.	Czy zaporę sieciową/firewall stosowany dla zabezpieczenia sieci wewnętrznej został indywidualnie skonfigurowany (nie są wykorzystywane ustawienia defaultowe)?		
74.	Czy podmiot przetwarzający udostępnia sieć Wi-Fi dla osób nieupoważnionych (np. gości)?		
	<i>Jeżeli nie – proszę przejść do pytania 76.</i>		
75.	Czy oprogramowanie wykorzystywane do przetwarzania danych osobowych jest dostępne z poziomu wydzielonej sieci Wi-Fi dla osób nieupoważnionych (np. gości)?		
76.	Czy sieć wewnętrzna podmiotu przetwarzającego została zabezpieczona np. z wykorzystaniem hasła lub identyfikacji adresu MAC?		
77.	Czy podmiot przetwarzający korzysta z innych rozwiązań zabezpieczających sieć wewnętrzną przed nieuprawnioną ingerencją lub dostępem? Jeżeli tak, w uwagach proszę napisać jakich.		
78.	Czy wyznaczono osobę odpowiedzialną za obserwację ruchu sieciowego lub czy opracowano i wdrożono zasady postępowania pozwalające na wykrywanie i reagowanie w przypadku peaków w ruchu sieciowym?		
<b>Zabezpieczenia organizacyjno-techniczne – poczta elektroniczna</b>			
<b>Lp.</b>	<b>Pytanie</b>	<b>Tak/Nie</b>	<b>Uwagi/komentarze</b>
79.	Czy podmiot przetwarzający opracował i wdrożył zasady korzystania z poczty elektronicznej przez pracowników?		
80.	Czy podmiot przetwarzający zezwala pracownikom na korzystanie poczty elektronicznej do celów prywatnych?		



<b>Zakres weryfikacji zgodności przetwarzania Danych Osobowych z postanowieniami Umowy o powierzeniu przetwarzania danych osobowych</b>			
<b>Uwaga: dane zawarte w ankiecie mogą stanowić tajemnicę przedsiębiorstwa</b>			
<b>Dane podmiotu</b>			
<b>Nazwa jednostki (pełna nazwa podmiotu, bez znaków dodatkowych typu „”):</b>		<b>NIP</b>	
<b>AKTYWNOŚĆ</b>	<b>KATEGORIA</b>	<b>PODKATEGORIA</b>	<b>STOPIEŃ WDROŻENIA</b>
<b>ZARZĄDZANIE (ZA)</b>	<b>Zespół odpowiedzialny za bezpieczeństwo (ZA.1)</b>	W jednostce jest dedykowana osoba odpowiedzialna za ochronę danych osobowych (ZA.1.1).	
		W jednostce wyznaczono Inspektora Ochrony Danych (ZA.1.2).	
		W jednostce jest dedykowana osoba odpowiedzialna za bezpieczeństwo fizyczne (ZA.1.3).	
		W jednostce jest dedykowana osoba odpowiedzialna za cyberbezpieczeństwo (ZA.1.4).	
		Osoby odpowiedzialne za cyberbezpieczeństwo, ochronę danych osobowych podlegają bezpośrednio pod kierownika jednostki (ZA.1.5).	
	<b>Działania zarządu jednostki (ZA.2)</b>	Dyrektor jednostki odbył szkolenie w zakresie cyberbezpieczeństwa w ciągu ostatniego roku (ZA.2.1). Podać datę szkolenia w dolnej części.	
		Dyrektor jednostki cyklicznie otrzymuje raport oceny ryzyka w jednostce (ZA.2.2).	
		Dyrektor jednostki wydał zarządzenie o zintegrowanym systemie zarządzania bezpieczeństwem w jednostce (ZA.2.3).	
		Dyrektor jednostki opublikował politykę bezpieczeństwa jednostki z uwzględnieniem cyberbezpieczeństwa (ZA.2.4).	
<b>DANE OSOBOWE (DO)</b>	<b>Współpraca z Administratorem (DO.1)</b>	Podmiot wdrożył odpowiednie środki techniczne i organizacyjne, które umożliwiają mu wsparcie Administratora w odpowiadaniu na żądania osób, których dane dotyczą, w zakresie realizacji ich praw wynikających z RODO (DO.1.1)	
		Podmiot wdrożył mechanizmy/procedury, umożliwiające bezzwłoczne zgłoszenie naruszenia bezpieczeństwa danych osobowych (DO.1.2)	
		Podmiot prowadzi rejestr naruszeń ochrony osobowych (DO.1.3)	
	<b>Środki organizacyjno-techniczne (DO.2)</b>	Osoby biorące udział przy przetwarzaniu zostały zobowiązane do zachowania tajemnicy (DO.2.1)	
		Podmiot stosuje fizyczne zabezpieczenia pomieszczeń/obszarów przetwarzania danych osobowych przed dostępem osób nieuprawnionych (DO.2.2)	
		Podmiot nadaje upoważnienia do przetwarzania danych osobowych (DO.2.3)	
		Podmiot prowadzi dokumentację ochrony danych osobowych (DO.2.4)	
		Podmiot prowadzi rejestr kategorii czynności przetwarzania (DO.2.5)	

		Dla każdego zasobu (fizycznego i elektronicznego), mającego wartość dla organizacji, wyznaczono osobę odpowiedzialną (Właściciela Zasobu) (DO.2.6)	
		Opracowano i wdrożono standardy dotyczące analizy ryzyka naruszenia praw podstawowych i wolności osób których dane dotyczą oraz utraty poufności, dostępności i integralności danych osobowych na każdym etapie cyklu życia systemu przetwarzającego te dane (DO.2.7)	
		Podmiot dokonuje oceny skutków przetwarzania dla ochrony danych osobowych (DO.2.8)	
		Ocena skutków przetwarzania dla ochrony danych osobowych jest konsultowana przez IOD (DO.2.9)	
		IOD monitoruje wykonanie skutków przetwarzania dla ochrony danych osobowych (DO.2.10)	
		Opracowano, wdrożono i zapewniono utrzymanie ciągłości działania systemu monitorowania zmian w obowiązujących przepisach prawa dotyczących zasad przetwarzania danych osobowych (DO.2.11)	
	<b>Ochrona danych w fazie projektowania oraz domyślna ochrona danych (DO.3)</b>	Opracowano i wdrożono standardy bezpiecznego wytwarzania oprogramowania (DO.3.1)	
		Opracowano i wdrożono standardy dotyczące zachowania zasady ochrony prywatności w fazie projektowania oprogramowania (DO.3.2)	
		Opracowano i wdrożono standardy dotyczące zachowania ochrony prywatności w ustawieniach domyślnych w fazie projektowania oprogramowania (DO.3.3)	
		Opracowano i zapewniono program szkoleń z zakresu zasad bezpiecznego wytwarzania oprogramowania (DO.3.4)	
		Opracowano i zapewniono program testów bezpieczeństwa oprogramowania (DO.3.5)	
		Wdrożono udokumentowaną politykę kontroli zmian obejmującą wymagania w zakresie zatwierdzenia, klasyfikacji, testowania i testowania planu back-out oraz rozdzielenie obowiązków pomiędzy wniosek, zatwierdzenie a wdrożenie (DO.3.6)	
	<b>Bezpieczeństwo operacji przetwarzania danych osobowych (DO.4)</b>	Dane osobowe zabezpiecza się przed utratą rozliczalności poprzez zastosowanie rozwiązań pozwalających przypisać określone działania konkretnej osobie lub systemowi informatycznemu (DO.4.1)	
		Dane osobowe zabezpiecza się przed utratą poufności za pomocą bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych (DO.4.2)	
		Dane osobowe zabezpiecza się przed utratą poufności za pomocą monitorowania poprawności działania oraz sposobu użycia bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych (DO.4.3)	
		Dane osobowe zabezpiecza się przed utratą poufności za pomocą przeprowadzanych i dokumentowanych okresowych (przynajmniej raz do roku) przeglądów dostępu wszystkich użytkowników, kont systemowych, kont testowych oraz kont ogólnych (DO.4.4)	
		Dane osobowe zabezpiecza się przed utratą poufności za pomocą wdrożenia mechanizmów kontroli sesji, w tym blokadę konta i wygaśnięcie sesji po ustalonym czasie (DO.4.5)	

		Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą poufności, dostępności i integralności poprzez zastosowanie fizycznej lub logicznej separacji danych (separacja danych) (DO.4.6)	
		Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą poufności, dostępności i integralności poprzez zastosowanie mechanizmów tworzących kopie danych w czasie rzeczywistym (replikacja danych) (DO.4.7)	
		Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą poufności, dostępności i integralności poprzez zastosowanie mechanizmów tworzących przyrostowe lub całościowe kopie bezpieczeństwa danych w ustalonym interwale czasowym (backup danych) (DO.4.8)	
		Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą poufności, dostępności i integralności poprzez zastosowanie mechanizmów i procedur przywracania danych, przełączania źródeł danych oraz odtwarzania kopii bezpieczeństwa danych (DO.4.9)	
		Dane osobowe przechowywane w bazach danych zabezpiecza się przed utratą integralności poprzez zastosowanie reguł spójności w zakresie semantycznym (definicja typu danych), zakresie encji (definicja kluczy podstawowych) oraz w zakresie referencyjnym (definicja kluczy obcych) (DO.4.10)	
		Dane osobowe zabezpiecza się przed utratą dostępności i integralności poprzez zastosowanie mechanizmów tworzących kopie robocze danych (DO.4.11)	
		Podmiot prowadzi ewidencję miejsc przetwarzania danych osobowych (DO.4.12)	
		Dane są przekazywane do państwa trzeciego lub organizacji międzynarodowej (EOG) (DO.4.13) Poddać w dolnej części nazwy państwa trzeciego lub organizacji międzynarodowej	
	<b>Dalsze powierzanie przetwarzania (DO.5)</b>	Podmiot dysponuje zgodą Administratora na dalsze powierzenie przetwarzania danych osobowych (DO.5.1)	
		Podmiot korzysta z usług innego podmiotu przetwarzającego (DO.5.2). Poddać w dolnej części nazwy takich podmiotów, czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą	
<b>ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI (SZBI)</b>	<b>Kroki podjęte w celu zapewnienia bezpieczeństwa informacji (SZBI.1)</b>	SZBI.1.1 - konieczność zapewnienia bezpieczeństwa informacji jest ujęta w strategii informatyzacji jednostki.	
		SZBI.1.2 – zidentyfikowano cele bezpieczeństwa informacji, określono sposoby ich realizacji oraz przypisano odpowiedzialność za ich realizację.	
		SZBI.1.3 – działania w zakresie bezpieczeństwa informacji podjęto przed rokiem 2021.	

		SZBI.1.4 – jednostka opracowała i przyjęła kompleksową politykę bezpieczeństwa informacji (PBI).	
		SZBI.1.5 – PBI opracowana w oparciu o właściwe standardy i dobre praktyki.	
		SZBI.1.6 – ostatni przegląd PBI jednostki przeprowadzono nie dawniej niż rok temu.	
	<b>Zarządzanie (SZBI.2) – Zasady, procedury i procesy zarządzania i monitorowania wymogów w zakresie regulacyjnym, prawnym, ryzyka ochrony środowiska i operacyjnym w organizacji są zrozumiałe i informują o zarządzaniu ryzykiem cyberbezpieczeństwa.</b>	SZBI.2.1 – Polityka cyberbezpieczeństwa organizacji jest przekazywana pracownikom w toku okresowych szkoleń stanowiskowych.	
		SZBI.2.2 – zidentyfikowano kluczowe aktywa informacyjne (zbiory danych/ systemy/ usługi).	
		SZBI.2.3 – aktywa zostały uwzględnione w rejestrze ryzyk jednostki	
		SZBI.2.4 – Zarządzanie w organizacji oraz zarządzanie ryzykiem odnoszą się do zagrożeń związanych z cyberbezpieczeństwem.	
	<b>Szacowanie ryzyka (SZBI.3) - Organizacja rozumie ryzyko cyberbezpieczeństwa dla działalności organizacyjnej (w tym misji, funkcji, wizerunku lub reputacji), zasobów organizacyjnych i osób.</b>	SZBI.3.1 – Podatności w zasobach są identyfikowane i dokumentowane.	
		SZBI.3.2 – w jednostce dokonuje się szacowania ryzyka związanego z zagrożeniami bezpieczeństwa informacji.	
		SZBI.3.3 – Zagrożenia, zarówno wewnętrzne jak i zewnętrzne, są identyfikowane i dokumentowane.	
		SZBI.3.4 – Zagrożenia, podatności, prawdopodobieństwo wystąpienia i skutki są używane do określania ryzyka.	
		SZBI.3.5 – Odpowiedzi na ryzyko są identyfikowane i priorytetyzowane.	
	<b>Strategia zarządzania ryzykiem (SZBI.4). Priorytety, ograniczenia, tolerancja ryzyk i założenia organizacji są określone i wspierają decyzję dotyczące ryzyka operacyjnego.</b>	SZBI.4.1 – Procesy zarządzania ryzykiem są ustanawiane , zarządzane i uzgadniane z dyrektorem jednostki.	
		SZBI.4.2 – w organizacji wdrożono system oceny ryzyka.	
	<b>Zarządzanie ryzykiem we współpracy zewnętrznej (SZBI.5) – Priorytety, ograniczenia, tolerancja ryzyk i założenia organizacji są określone i wykorzystywane do wspierania decyzji o ryzyku związanym z zarządzaniem ryzykiem łańcucha dostaw. Organizacja ustanowiła i wdrożyła procesy identyfikacji, szacowania i zarządzania ryzykiem łańcucha dostaw.</b>	SZBI.5.1 – Procesy zarządzania ryzykiem cyberbezpieczeństwa są identyfikowane, ustanawiane, oceniane.	
		SZBI.5.2 – Partnerzy zewnętrzni i dostawcy w zakresie systemów informacyjnych, komponentów i usług są identyfikowani, priorytetyzowani i oceniani za pomocą procesu oceny ryzyka cyberbezpieczeństwa.	
		SZBI.5.3 – Umowy z dostawcami i partnerami zewnętrznymi są wykorzystywane do wdrażania odpowiednich środków dla osiągnięcia celów programu cyberbezpieczeństwa.	
		SZBI.5.4 – Dostawcy i partnerzy zewnętrzni są stale oceniani przy użyciu audytów, wyników, testów lub innych form oceny w celu potwierdzenia, że wywiązują się ze swoich zobowiązań w zakresie bezpieczeństwa.	
<b>OCHRONA (OCH)</b>	<b>Zarządzanie tożsamościami, uwierzytelnianie i kontrola dostępu (OCH1)</b>	OCH.1.1 – W jednostce wdrożono system zarządzania tożsamością i uprawnieniami.	
		OCH.1.2 – Fizyczny dostęp do zasobów jest zarządzany, chroniony.	
		OCH.1.3 – Dostęp zdalny jest zarządzany.	

		OCH.1.4 – Uprawnienia dostępu i autoryzacja są zarządzane z uwzględnieniem zasady najniższych uprawnień i rozdzielania obowiązków.	
		OCH.1.5 – integralność sieci jest chroniona (np. poprzez segregację sieci czy jej segmentację).	
		OCH.1.6. – weryfikacja dostępu opiera się o MFA (uwierzelnianie wieloskładnikowe) i jest wykorzystywane aktualnie.	
	<b>Świadomość podnoszenia kompetencji (OCH.2)</b>	OCH.2.1 – w jednostce wdrożono system zarządzania tożsamością i uprawnieniami.	
		OCH.2.2 – użytkownicy ze zwiększonymi uprawnieniami rozumieją swoją rolę i obowiązki.	
		OCH.PZ.3 – Podmioty zewnętrzne (np. dostawcy, klienci, partnerzy) rozumieją swoje role i obowiązki.	
		OCH.2.3 – Kadra kierownicza wyższego szczebla rozumie swoje role i obowiązki.	
		OCH.2.4 – Personel cyberbezpieczeństwa oraz bezpieczeństwa fizycznego rozumie swoje role i obowiązki.	
	<b>Bezpieczeństwo danych (OCH.3)</b>	OCH.3.1 – Dane w spoczynku są chronione.	
		OCH.3.2 – Przesyłane dane są chronione.	
		OCH.3.3 – Zasoby są formalnie zarządzane podczas usuwania, przenoszenia, dysponowania.	
		OCH.3.4 – Utrzymywana jest odpowiednia zdolność do zapewnienia dostępności.	
		OCH.3.5 – Wdrożono mechanizmy ochrony przed wyciekami danych.	
	<b>Bezpieczeństwo kopii zapasowych. Plany reagowania na zagrożenia (OCH.4)</b>	OCH.4.1 – Kopie zapasowe informacji są sporządzane, utrzymywane i testowane	
		OCH.4.2 – Dostęp do kopii zapasowych jest dodatkowo chroniony.	
		OCH.4.3 - Dane są niszczone zgodnie z funkcjonującymi politykami	
		OCH.4.4 – Opracowano plan backupu i administrowania kopii zapasowych.	
		OCH.4.5 - Organizacja posiada i zarządza planami reagowania (w zakresie reagowania na incydenty, ciągłości działania) oraz planami odtwarzania (w zakresie odtwarzania po incydencie i po awarii).	
		OCH.4.6 – plany reagowania i odtwarzania są weryfikowane i testowane	
		Och.4.7 - Opracowano i wdrożono plan zarządzania podatnościami .	
	<b>Technologia ochronna (OCH.5)</b>	OCH.TO-1- Zapisy logów / inspekcji są określone, dokumentowane, wdrażane i sprawdzane zgodnie z politykami.	
		OCH.TO-2 - nośniki wymienne są chronione, a ich stosowanie ograniczone zgodnie z politykami.	
		OCH.TO-3 - Zasada najmniejszej funkcjonalności jest wdrożona poprzez odpowiednią konfigurację systemów tak, by posiadały tylko niezbędne możliwości.	
		OCH.TO-4 - Łącza komunikacyjne do Internetu są chronione.	



		OCH.TO-5 - Odpowiednie mechanizmy jak np. funkcje równoważenia obciążenia, hotswap) są wdrożone w celu osiągnięcia wymagań dotyczących odporności w normalnych i niekorzystnych sytuacjach.	
<b>ZDARZENIA I MONITORING (CM)</b>	<b>Anomalie i zdarzenia (CM.1)</b>	CM.1.1 – Wykryte zdarzenia są analizowane aby zrozumieć cele i metody ataku.	
		CM.1.2 – Dane o zdarzeniach są pozyskiwane oraz korelowane z wielu źródeł i czujników.	
	Ciągłe monitorowanie bezpieczeństwa (CM.2)	CM.2.1 - Sieć jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa (SIEM).	
		CM.2.2 – Środowisko fizyczne jest monitorowane w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa.	
		CM.2.3 - Aktywność personelu jest monitorowana w celu wykrycia potencjalnych zdarzeń związanych z cyberbezpieczeństwem.	
		CM.2.4 – Złośliwy kod jest wykrywany	
		CM.2.5 – Nieautoryzowany kod mobilny jest wykrywany (np. Activex, JavaScript)	
		CM.2.6 – Aktywność zewnętrznego dostawcy usług jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa.	
		CM.2.7 – Przeprowadza się monitorowanie pod kątem nieautoryzowanego personelu, połączeń, urządzeń i oprogramowania.	
		CM.2.8 – Przeprowadza się skanowanie podatności.	
<b>REAGOWANIE (RE)</b>	<b>Planowanie reagowania (RE)</b>	RE.1 – Plan reagowania jest realizowany w trakcie lub po incydencie.	
	<b>Komunikacja (KO)</b>	KO.1 – Personel zna swoje role i kolejność operacji, na wypadek konieczności reagowania.	
		KO.2 – Incydenty są zgłaszane zgodnie z ustalonymi kryteriami.	
		KO.3 – Informacje są udostępniane zgodnie z planami reagowania.	
		KO.4 – Koordynacja z zainteresowanymi stronami jest prowadzona w sposób zgodny z planami reagowania.	
		KO.5 – Dobrowolna wymiana informacji z zewnętrznymi podmiotami jest prowadzona w celu osiągnięcia szerszej świadomości sytuacyjnej w zakresie cyberbezpieczeństwa.	
	<b>Mitygacja (MI)</b>	MI.1 – Incydenty są opanowywane.	
		MI.2 – Incydenty są mitygowane.	
		MI.3 – Nowo zidentyfikowane podatności są mitygowane lub dokumentuje się akceptację ryzyka związanego z nimi.	
	<b>Udoskonalanie (UD)</b>	UD.1 – Plany reagowania uwzględniają wyciągnięte wnioski.	
		UD.2 – Strategie reagowania są aktualizowane.	
<b>ODTWARZANIE (OD)</b>	<b>Planowanie odtwarzania (OD.1)</b>	OD.1.1 – Plan odtwarzania jest realizowany w trakcie lub po incydencie cyberbezpieczeństwa.	
	<b>aktualizacja (OD.2)</b>	OD.2.1 – Plany odtwarzania zawierają wyciągnięte dotychczas wnioski	
		OD.2.2 – Strategie odtwarzania są aktualizowane.	
<b>INFRASTRUKTURA (IN)</b>	<b>Sieć LAN (IN.1)</b>	IN.1.1 – przełączniki klasy enterprise, wsparcie.	

		IN.1.2 – segmentacja sieci.	
	<b>Ochrona brzegowa (IN.2)</b>	IN.2.1 – Firewall klasy enterprise, aktualne wsparcie, aktualizacje na bieżąco.	
		IN.2.2 – połączenia VPN oraz certyfikaty dla wszystkich użytkowników.	
	<b>poczta (IN.3)</b>	IN.3.1 – serwer poczty.	
		IN.3.2 – wdrożony SANDBOX	
		IN.3.3 – wdrożony MFA dla wszystkich użytkowników usług pocztowych i aktualnie wykorzystywany.	
	<b>wirtualizacja (IN.4)</b>	IN.4.1 – serwery wirtualne.	
		IN.4.2 – wsparcie i aktualizacje.	
	<b>kopia zapasowa (IN.5)</b>	IN.5.1 – Kopia odmiejszczona.	
		IN.5.2 – Napęd taśmowy (biblioteka taśmowa).	
		IN.5.3 – System kopii zapasowej izolowany od środowisk produkcyjnych (wydzielane sieci, urządzenia składowania danych inne niż produkcyjne).	
		IN.5.4 – Istnieją harmonogramy wykonywania kopii bezpieczeństwa dla wszystkich systemów produkcyjnych.	
		IN.5.5 - Kopie bezpieczeństwa okresowo odtwarzane. Sprawdzane działanie odtworzonego systemu aplikacji.	
	<b>systemy bezpieczeństwa (IN.6)</b>	IN.6.1 SIEM/SOAR (Security Information and Event Management /Security Orchestration, Automation and Response)	
		IN.6.2 DLP (Data Loss Prevention/Data Loss Protection)	
		IN.6.3 NAC (Network Access Control)	
		IN.6.4 WAF (Web Application Firewall)	
		IN.6.5 DAM (Database Activity Monitoring)	
		IN.6.6 EDR/XDR (Endpoint Detection and Response/eXtended Detection and Response)	
		IN.6.7 DNS Protection	
		IN.6.8 IPS/IDS (Intrusion Detection System/Intrusion Prevention System)	
		IN.6.9 Antivirus	
		IN.6.10 SOC (Security Operations Center)	
	<b>urządzenia specjalizowane, specyficzne dla prowadzonej działalności (IN.7)</b>		
<b>TELEKOMIUNIKACJA</b>	<b>typ łącza telekomunikacyjnego</b>		
	<b>przepustowość (w przypadku łącz</b>		

	niesymetrycznych suma download +upload)		
	usługa antyDDos		
	firewall dostarczony przez operatora i przez operatora zarządzany		
	firmowe telefony komórkowe		
	telefonía VoIP wewnątrz jednostki		
	łącze głosowe		
	łącze głosowe awaryjne, niezależne od zasilania lokalnego		
	centrałka telefoniczna		
<b>ZASILANIE AWARYJNE</b>	UPS na stanowisku roboczym		
	Wszystkie serwerownie zasilane z UPS w czasie rozruchu generatora		
	Wszystkie serwery z zasilaczami redundantnymi		
	Generator awaryjny na potrzeby wszystkich serwerowni		
	SZR załączający generator awaryjny w trakcje pracy na UPS		
	Zatankowany zbiornik paliwa wystarczy		
	Zasilanie jednostki z dwóch stacji transformatorowych SN/NN		
	Awaryjne zasilanie we wszystkich serwerowniach		

.....

Data; kwalifikowany podpis elektroniczny lub podpis  
zaufany lub podpis osobisty

Załącznik nr 4 do SWZ

postępowanie numer DOA.201.2.2026

### Dane Wykonawcy

.....  
Nazwa

.....  
Adres siedziby

.....  
NIP / REGON

.....  
Osoba do kontaktu, telefon / e-mail

### FORMULARZ CENOWY

Przedmiot zamówienia – Wdrożenie i świadczenie usługi SOC (Security Operation Center), zostanie zrealizowany za następujące ceny:

Lp.	Przedmiot zamówienia	Udział % w łącznej cenie	Cena netto w PLN	VAT w PLN	Cena brutto w PLN
1.	Wdrożenia i uruchomienie Usługi SOC –jednorazowe wynagrodzenie	<b>60%±5%</b>			
2.	Świadczenie usługi SOC jako usługi (Security Operations Center as a Service) ( <b>łącznie kwota wynagrodzenia miesięcznego za okres 12 miesięcy</b> )	<b>40%±5%</b>			
3.	<b>Suma (1+2)</b>				

Miesięczne wynagrodzenie w wysokości netto: ..... zł (słownie:  
..... złotych..... /100 gr netto), VAT:  
..... zł (słownie: .....), brutto: .....zł  
(słownie:..... złotych ...../100 gr brutto)

**Uwaga**

Formularz cenowy Wykonawca składa wraz z Interaktywnym formularzem ofertowym, wypełnianym za pośrednictwem Platformy, w którym poda cenę brutto oferty za wykonanie przedmiotu zamówienia. Cena brutto oferty podana w Interaktywnym formularzu oferty powinna być równa wartości brutto podanej przez Wykonawcę w Formularzu cenowy.

.....

Data; kwalifikowany podpis elektroniczny lub podpis  
zaufany lub podpis osobisty



Urząd Ochrony Danych  
Osobowych  
ul. Stanisława Moniuszki 1A  
00-014 Warszawa

Wykonawca:

.....

.....

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP, KRS/CEiDG)

reprezentowany przez:

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

**Oświadczenia wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie  
zamówienia**

**UWZGLĘDNIAJĄCE PRZESŁANKI WYKLUCZENIA Z ART. 7 UST. 1 USTAWY o  
szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na  
Ukrainę oraz służących ochronie bezpieczeństwa narodowego**

**składane na podstawie art. 125 ust. 1 Pzp**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. Wdrożenie i świadczenie usługi SOC (Security Operation Center) oświadczam, co następuje:  
OŚWIADCZENIA DOTYCZĄCE PODSTAW WYKLUCZENIA:

1. Oświadczam, że nie podlegam/nie podlegam<sup>1</sup> wykluczeniu z postępowania na podstawie art.108 ust. 1 pkt 1-6 oraz art. 109 ust. 1 pkt 4, 8 Pzp.
2. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie 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<sup>2</sup>.

<sup>1</sup> Niepotrzebne skreślić.

<sup>2</sup> Zgodnie z treścią 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, zwanej dalej „ustawą”, z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie Pzp wyklucza się:

**OŚWIADCZENIE DOTYCZĄCE WARUNKÓW UDZIAŁU W POSTĘPOWANIU:**

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w Specyfikacji Warunków Zamówienia oraz Ogłoszeniu o zamówieniu.

**INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZDOLNOŚCIACH LUB SYTUACJI PODMIOTÓW UDOSTĘPNIAJĄCYCH ZASOBY:**

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w Specyfikacji Warunków Zamówienia oraz Ogłoszeniu o zamówieniu, polegam na zdolnościach lub sytuacji następującego/ych podmiotu/ów udostępniających zasoby: (wskazać nazwę/y podmiotu/ów)..... w następującym zakresie: .....

(określić odpowiedni zakres udostępnianych zasobów dla wskazanego podmiotu).

1) wykonawcę oraz uczestnika konkursu 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;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu 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;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości, 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 2022 r., 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.

Urząd Ochrony Danych Osobowych  
ul. Stanisława Moniuszki 1A  
00-014 Warszawa

[www.uodo.gov.pl](http://www.uodo.gov.pl)

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

**INFORMACJA DOTYCZĄCA DOSTĘPU DO PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:**

Wskazuję następujące podmiotowe środki dowodowe, które można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, oraz dane umożliwiające dostęp do tych środków:

1).....

(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)

2).....

(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)

Oświadczenie Wykonawca składa wraz z ofertą.

.....

Data; kwalifikowany podpis elektroniczny lub podpis  
zaufany lub podpis osobisty

**Załącznik nr 6 do SWZ**

Wykonawca:

.....  
.....  
.....

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP, KRS/CEiDG)

reprezentowany przez:

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

**Wykaz usług spełniających wymagania zawarte w Rozdziale XVIII SWZ**

Składając Ofertę w postępowaniu o udzielenie zamówienia publicznego pn.  
Wdrożenie i świadczenie usługi SOC (Security Operation Center) oświadczam, że  
zrealizowaliśmy następującą usługę:

Lp.	Odbiorca/ Zamawiający	Przedmiot zamówienia	Termin wykonania	
			Rozpoczęcie data, m-c, rok	Zakończenie data, m-c, rok
1.				

Uwaga!

– dowody określające czy te usługi zostały wykonane lub są wykonywane należycie. Dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były lub są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy

.....

Data; kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty

Wykonawca:

.....

.....

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP, KRS/CEiDG)

reprezentowany przez:

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

**WYKAZ OSÓB**  
**skierowanych przez Wykonawcę do realizacji zamówienia publicznego**

Przedstawiamy wykaz osób (*dla wykazania spełnienia warunku udziału w postępowaniu*), skierowanych przez Wykonawcę do realizacji zamówienia, które będą uczestniczyć w jego wykonywaniu:

Lp.	Nazwisko i imię	Posiadane Certyfikaty	Rola/funkcja w realizacji zamówienia
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			

10.			
11.			
12.			
13.			
14.			
15.			

.....  
Data; kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty