Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

ZAMAWIAJĄCY:

GMINA MIEJSKA CIECHOCINEK

zaprasza do złożenia oferty w postępowaniu o udzielenie zamówienia publicznego na realizację zadania pn.

„Dostawa sprzętu i oprogramowania dla Gminy Miejskiej Ciechocinek."

Zamówienie jest realizowane w ramach konkursu grantowego „Cyberbezpieczny Samorząd" realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Postępowanie prowadzone jest przy użyciu środków komunikacji elektronicznej. Składanie ofert następuje za pośrednictwem platformy zakupowej dostępnej pod adresem internetowym: https://ezamowienia.gov.pl

Identyfikator postępowania nadany przez platformę zakupową:

ocds-148610-c4d23197-530a-4500-997c-b9574e45aadd

Nr postępowania: BSR – ZP.271.3.2026

Z up. BURMISTRZA
mgr Joanna Bryżałowska
Zastępca Burmistrza

Sprawę prowadzi:
Ewelina Kurtys-Żak

Ciechocinek, 16.02.2026 r.

Oznaczenie postępowania: BSR-ZP.271.3.2026

I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

Gmina Miejska Ciechocinek

ul. Mikołaja Kopernika 19

87-720 Ciechocinek

Tel.: 54 416 18 00

Adres e-mail: ratusz@ciechocinek.pl

Identyfikator postępowania: ocds-148610-c4d23197-530a-4500-997c-b9574e45aadd

Adres strony internetowej, na której jest prowadzone postępowanie i na której będą dostępne wszelkie dokumenty związane z prowadzoną procedurą: https://ezamowienia.gov.pl/mp-client/tenders/ocds-148610-c4d23197-530a-4500-997c-b9574e45aadd

II. TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie prowadzone jest w trybie podstawowym, o którym mowa w art. 275 pkt 1 p.z.p.
2. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
3. Szacunkowa wartość przedmiotowego zamówienia nie przekracza progów unijnych o jakich mowa w art. 3 ustawy p.z.p.
4. Zgodnie z art. 310 pkt 1 p.z.p. Zamawiający przewiduje możliwość unieważnienia przedmiotowego postępowania, jeżeli środki, które Zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostały mu przyznane.
5. Zamawiający nie przewiduje aukcji elektronicznej.
6. Zamawiający nie przewiduje złożenia oferty w postaci katalogów elektronicznych.
7. Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.
8. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94 p.z.p.
9. Zamawiający nie stawia wymagań związanych z realizacją zamówienia w zakresie zatrudnienia przez wykonawcę lub podwykonawcę na podstawie stosunku pracy osób wykonujących wskazane przez zamawiającego czynności w zakresie realizacji zamówienia,

jeżeli wykonanie tych czynności polega na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2020 r. poz. 1320).

10. Zamawiający nie określa dodatkowych wymagań związanych z zatrudnianiem osób, o których mowa w art. 96 ust. 2 pkt 2 p.z.p.

III. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiot zamówienia obejmuje zakup i wdrożenie rozwiązań sprzętowych i programowych w zakresie bezpieczeństwa sieci i systemów informatycznych dla Urzędu i jednostek podległych.
2. Kody CPV:
   1) 37453300-1 – Dyski
   2) 48820000-2 – Serwery
   3) 32420000-3 – Urządzenia sieciowe
   4) 35120000-1 – Systemy i urządzenia nadzoru i bezpieczeństwa
   5) 48000000-8 – Pakiety oprogramowania i systemy informatyczne
   6) 72260000-5 – Usługi w zakresie oprogramowania
   7) 72250000-2 – Usługi w zakresie konserwacji i wsparcia systemów
3. Szczegółowy opis przedmiotu zamówienia zawarty jest w **Załączniku nr 4 do SWZ**
4. Zamawiający nie dopuszcza możliwość składanie ofert częściowych w ramach jednego postępowania.
5. Zamawiający nie podzielił zamówienia na części ze względu na fakt, iż integralność i spójność całego systemu cyberbezpieczeństwa jest kluczowa dla zapewnienia wysokiego poziomu ochrony danych i infrastruktury informatycznej gminy. Podział zamówienia na części mógłby prowadzić do problemów z kompatybilnością oraz trudnościami w zarządzaniu i integracji różnych systemów i urządzeń dostarczanych przez różnych dostawców. Dodatkowo, jeden wykonawca jest w stanie lepiej zagwarantować zgodność technologiczną oraz spójne wsparcie techniczne dla całego systemu, co jest szczególnie istotne w kontekście cyberbezpieczeństwa, gdzie szybkość reakcji i kompleksowe podejście do problemów są niezbędne. Ponadto, z punktu widzenia administracyjnego i organizacyjnego, zarządzanie jednym kontraktem jest prostsze i bardziej efektywne, co

przekłada się na oszczędność czasu i zasobów. Uwzględniając powyższe argumenty, zdecydowano, że niepodzielenie zamówienia na części jest rozwiązaniem najkorzystniejszym zarówno z perspektywy technicznej, jak i organizacyjnej.

IV. WIZJA LOKALNA

Zamawiający informuje, że nie jest wymagane odbycie wizji lokalnej.

V. PODWYKONAWSTWO

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).
2. Zamawiający, działając zgodnie z art. 60 ust. 2 ustawy Prawo zamówień publicznych, zastrzega obowiązek osobistego wykonania przez Wykonawcę następujących kluczowych części zamówienia:
   a. konfiguracja i uruchomienie sprzętu serwerowego,
   b. instalacja oraz konfiguracja systemów informatycznych,
   c. wdrożenie rozwiązań w zakresie cyberbezpieczeństwa.
3. Dostawa sprzętu i oprogramowania może zostać powierzona podwykonawcom, jednak Wykonawca ponosi pełną odpowiedzialność za należyte wykonanie całości zamówienia.
4. Zastrzeżenie wynika z konieczności zapewnienia pełnej odpowiedzialności Wykonawcy za zgodność technologiczną, bezpieczeństwo danych oraz spójność wdrożenia.
5. Zastrzeżenie wynika z konieczności zapewnienia pełnej odpowiedzialności Wykonawcy za zgodność technologiczną, bezpieczeństwo danych oraz spójność wdrożenia. Wykonawca może powierzyć podwykonawcom realizację pozostałych elementów zamówienia, jednak ponosi pełną odpowiedzialność za należyte wykonanie całości przedmiotu zamówienia.
6. Zamawiający podkreśla, że osobiste wykonanie kluczowych części zamówienia ma na celu:
   a. zagwarantowanie kompatybilności sprzętu i oprogramowania,
   b. zapewnienie jednolitego standardu wdrożenia,
   c. minimalizację ryzyka związanego z bezpieczeństwem informacji,
   d. usprawnienie procesu zarządzania i serwisowania systemu.
7. W pozostałym zakresie Wykonawca może korzystać z podwykonawców, zgodnie z warunkami określonymi w niniejszej SWZ.

8. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.

VI. TERMIN WYKONANIA ZAMÓWIENIA

1. Termin wykonania zamówienia: do 40 dni kalendarzowych począwszy od dnia zawarcia umowy.

VII. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na zasadach określonych w Rozdziale VIII SWZ, oraz spełniają określone przez Zamawiającego warunki udziału w postępowaniu.
2. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki dotyczące:
   1) **zdolności do występowania w obrocie gospodarczym:**
      Zamawiający nie stawia warunku w powyższym zakresie.
   2) **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:**
      Zamawiający nie stawia warunku w powyższym zakresie.
   3) **sytuacji ekonomicznej lub finansowej:**

Wykonawca spełni warunek, jeżeli wykaże, że jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na łączną kwotę równą co najmniej: 600.000,00 zł.

   4) **zdolności technicznej lub zawodowej:**
      a) **Doświadczenie**

Zamawiający wymaga, aby Wykonawca wykazał się należytym doświadczeniem w realizacji dostaw o charakterze i złożoności porównywalnej z przedmiotem niniejszego zamówienia. W szczególności Wykonawca musi udokumentować, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, zrealizował:

jedno zamówienie (umowę) polegające na dostawie oraz wdrożeniu systemu zabezpieczenia sieci, o wartości nie mniejszej niż 50 000,00 zł brutto oraz jedno zamówienie

(umowę) polegające na dostawie serwerów, o wartości nie mniejszej niż 100 000,00 zł brutto.

W celu potwierdzenia spełniania powyższego warunku Wykonawca zobowiązany jest do przedstawienia wykazu wykonanych zamówień wraz z podaniem:

- przedmiotu zamówienia,
- daty wykonania,
- odbiorcy (zamawiającego),

oraz dołączenia dowodów potwierdzających, że zamówienia te zostały wykonane należycie, w szczególności w postaci referencji, protokołów odbioru lub innych dokumentów wystawionych przez podmiot, na rzecz którego zamówienie było realizowane.

b) Potencjał kadrowy

Wykonawca wykaże, że dysponuje lub będzie dysponował na czas realizacji zamówienia osobami zdolnymi do wykonania zamówienia, tj. że skieruje do realizacji przedmiotu zamówienia co najmniej jedną osobę posiadającą odpowiednie kwalifikacje, potwierdzone ważnym certyfikatem producenta oferowanego rozwiązania w zakresie oferowanych urządzeń klasy UTM, na poziomie co najmniej profesjonalnym (Professional) lub równoważnym, uprawniającym do samodzielnej instalacji, konfiguracji oraz utrzymania urządzeń.

Certyfikat musi być ważny (aktywny) co najmniej na dzień składania ofert oraz musi zachować ważność przez cały okres realizacji zamówienia.

W przypadku, gdy okres ważności certyfikatu upływa w trakcie realizacji zamówienia, Wykonawca zobowiązany jest zapewnić jego odnowienie lub wskazać inną osobę spełniającą wymagania, nie później niż przed upływem ważności certyfikatu, bez dodatkowych kosztów dla Zamawiającego.

Certyfikat musi być wystawiony przez producenta oferowanego rozwiązania UTM. Niedopuszczalne jest wykazanie certyfikatu producenta innego niż producent oferowanych urządzeń.

Przez certyfikat na poziomie profesjonalnym Zamawiający rozumie certyfikat znajdujący się w strukturze certyfikacyjnej producenta powyżej poziomu podstawowego (Associate/Entry/Foundational lub równoważnego).

Wykaz osób skierowanych do realizacji zamówienia, wraz z informacjami na temat posiadanych kwalifikacji zawodowych, uprawnień oraz doświadczenia, stanowi podmiotowy środek dowodowy i składany jest na wezwanie Zamawiającego.

Do wykazu osób Wykonawca zobowiązany jest dołączyć kopie certyfikatów potwierdzających spełnienie wymagań oraz – jeżeli dotyczy – dokument potwierdzający aktualny status certyfikatu w systemie producenta.

3. Zamawiający, w stosunku do Wykonawców wspólnie ubiegających się o udzielenie zamówienia, w odniesieniu do warunku dotyczącego zdolności technicznej lub zawodowej – dopuszcza łączne spełnianie warunku przez Wykonawców.
4. Zamawiający może na każdym etapie postępowania, uznać, że wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez wykonawcę sprzecznych interesów, w szczególności zaangażowanie zasobów technicznych lub zawodowych wykonawcy w inne przedsięwzięcia gospodarcze wykonawcy może mieć negatywny wpływ na realizację zamówienia.

VIII. PODSTAWY WYKLUCZENIA Z POSTĘPOWANIA

1. Z postępowania o udzielenie zamówienia wyklucza się Wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych:
   1) w art. 108 ust. 1 p.z.p.;
   2) w art. 109 ust. 1 pkt 4-7 p.z.p.;

   Wykluczenie Wykonawcy następuje z uwzględnieniem z art. 111 p.z.p.
   3) w art. 5k 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 z 2014, poz. 229.1 ze zm.);
   4) w art. 7 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (tekst jedn. Dz.U. z 2025 r., poz. 514 ze zm.)

IX. OŚWIADCZENIA I DOKUMENTY, JAKIE ZOBOWIĄZANI SĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ WYKAZANIA BRAKU PODSTAW WYKLUCZENIA (PODMIOTOWE ŚRODKI DOWODOWE)

1. Do oferty Wykonawca zobowiązany jest dołączyć:
   1) aktualne na dzień składania ofert oświadczenie o spełnianiu warunków udziału w postępowaniu oraz o braku podstaw do wykluczenia z postępowania (art. 125 ust. 1 p.z.p.)– **Załącznik nr 2 do SWZ**;
   2) wypełniony formularz OPZ w kolumnie spełnia/ nie spełnia – **Załącznik nr 4 do OPZ**
2. Informacje zawarte w oświadczeniu, o którym mowa w pkt 1. 1) stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
3. Zamawiający wzywa wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych, jeżeli wymagał ich złożenia w ogłoszeniu o zamówieniu lub dokumentach zamówienia, aktualnych na dzień złożenia podmiotowych środków dowodowych.
4. Podmiotowe środki dowodowe wymagane od wykonawcy obejmują:
   1) odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
   2) wykaz dostaw zrealizowanych nie wcześniej niż w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, porównywalnych z zakresem stanowiącymi przedmiot zamówienia, wraz z podaniem ich rodzaju, wartości, daty, miejsca wykonania i podmiotów, na rzecz których dostawy te zostały wykonane, oraz załączeniem dowodów określających czy zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego roboty budowlane były wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – inne odpowiednie dokumenty - **Załącznik nr 5 do SWZ**

3) wykaz osób skierowanych do realizacji zamówienia wraz z informacjami na temat posiadanych kwalifikacji zawodowych, uprawnień oraz doświadczenia. Do wykazu osób Wykonawca zobowiązany jest załączyć dokumenty potwierdzające posiadanie wymaganych certyfikatów technicznych – **Załącznik nr 9 do SWZ**

4) dokumenty potwierdzające, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia.

5. W zakresie nieuregulowanym p.z.p. lub niniejszą SWZ do oświadczeń i dokumentów składanych przez Wykonawcę w postępowaniu zastosowanie mają w szczególności przepisy 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 (Dz.U. z 2020 r., poz. 2415 z późn. zm.) oraz 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 (Dz.U. z 2020 r., poz. 2452 z późn zm.).

X. POLEGANIE NA ZASOBACH INNYCH PODMIOTÓW

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. W odniesieniu do warunków dotyczących doświadczenia, wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają świadczenie do realizacji którego te zdolności są wymagane.
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. Wzór oświadczenia stanowi **Załącznik nr 3 do SWZ.**
4. Zamawiający ocenia, czy udostępniane wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez wykonawcę spełniania

warunków udziału w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.

5. Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, zamawiający żąda, aby wykonawca w terminie określonym przez zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
6. **UWAGA:** Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
7. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniem, o którym mowa w Rozdziale X ust. 1 SWZ, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim wykonawca powołuje się na jego zasoby, zgodnie z katalogiem dokumentów określonych w Rozdziale X SWZ.

XI. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA (SPÓŁKI CYWILNE/ KONSORCJA)

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.
2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale X ust. 1 SWZ, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

3. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które roboty budowlane/dostawy/usługi wykonają poszczególni wykonawcy.
4. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.

XII. SPOSÓB KOMUNIKACJI ORAZ WYJAŚNIENIA TREŚCI SWZ

1. W postępowaniu o udzielenie zamówienia publicznego komunikacja między Zamawiającym a wykonawcami odbywa się przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem https://ezamowienia.gov.pl.
2. Korzystanie z Platformy e-Zamówienia jest bezpłatne.
3. Adres strony internetowej prowadzonego postępowania: https://ezamowienia.gov.pl/mp-client/tenders/ocds-148610-c4d23197-530a-4500-997c-b9574e45aadd
4. Postępowanie można wyszukać również ze strony głównej Platformy e-Zamówienia (przycisk „Przeglądaj postępowania/konkursy").
5. Identyfikator (ID) postępowania na Platformie e-Zamówienia: ocds-148610-c4d23197-530a-4500-997c-b9574e45aadd
6. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać dostęp do konta na Platformie e-Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej https://ezamowienia.gov.pl oraz informacje zamieszczone w zakładce „Centrum Pomocy".
7. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Centrum pomocy platformy e-Zamówienia pod adresem https://ezamowienia.gov.pl/pl/komponent-edukacyjny/.
8. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie e-Zamówienia ani logowania.
9. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe

odwzorowania) musi być zgodny 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 konkursie (Dz.U. z 2020 r., poz. 2452 z późn.zm.).

10. Dokumenty elektroniczne, o których mowa w § 2 ust. 1 rozporządzenia wskazanego w pkt 7 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 (Dz.U. z 2024 r., poz. 773) z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki.
11. W przypadku formatów, o których mowa w art. 66 ust. 1 ustawy, ww. regulacje nie będą miały bezpośredniego zastosowania.
12. Informacje, oświadczenia lub dokumenty, inne niż wymienione w § 2 ust. 1 rozporządzenia, o którym mowa w pkt 7 , przekazywane w postępowaniu sporządza się w postaci elektronicznej:
    - w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (i przekazuje się jako załącznik), lub
    - jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej (np. w treści wiadomości e-mail lub w treści „Formularza do komunikacji").
13. 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 2022 r. poz. 1233 z późn. zm.) 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".
14. Komunikacja w postępowaniu, z wyłączeniem składania ofert/wniosków o dopuszczenie do udziału w postępowaniu, 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").

15. W przypadku załączników, które są zgodnie z p.z.p. lub rozporządzeniem Prezesa Rady Ministrów, o którym mowa w pkt 7 opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być opatrzone, zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby, podpisem zewnętrznym lub wewnętrznym. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) dodaje się do przesyłanej wiadomości uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
16. 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 e-Zamówienia.
17. Wszystkie wysłane i odebrane w postępowaniu przez wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce „Komunikacja".
18. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji" wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
19. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia.
20. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego poprzez formularz udostępniony na stronie internetowej https://ezamowienia.gov.pl w zakładce „Zgłoś problem".

21. Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres e-mail: zamowieniapubliczne-fs@ciechocinek.pl (nie dotyczy składania ofert).
22. Za datę przekazania oferty, oświadczenia, o którym mowa w art. 125 ust. 1 p.z.p., podmiotowych środków dowodowych, przedmiotowych środków dowodowych oraz innych informacji, oświadczeń lub dokumentów, przekazywanych w postępowaniu, przyjmuje się datę ich przekazania na platformę e-Zamówienia.
23. Osobą uprawnioną do porozumiewania się z Wykonawcami jest:
    1) w zakresie proceduralnym:
       Pani Ewelina Kurtys-Żak tel. 54 281 86 22;
       e-mail:zamowieniapubliczne-fs@ciechocinek.pl
    2) w zakresie merytorycznym:
       Pan Rafał Podczaski tel. 54 281 86 47
       e-mail: bip@ciechocinek.pl
24. W korespondencji kierowanej do Zamawiającego Wykonawcy powinni posługiwać się numerem przedmiotowego postępowania.
25. Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie treści SWZ
26. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania odpowiednio ofert, pod warunkiem że wniosek o wyjaśnienie treści SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania odpowiednio ofert.
27. Jeżeli zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w pkt 26 powyżej, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w pkt 26 powyżej, zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
28. Przedłużenie terminu składania ofert, o których mowa w ust. 12, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.

XIII. OPIS SPOSOBU PRZYGOTOWANIA OFERT ORAZ WYMAGANIA FORMALNE DOTYCZĄCE SKŁADANYCH OŚWIADCZEŃ I DOKUMENTÓW

1. Wykonawca może złożyć tylko jedną ofertę.
2. Treść oferty musi odpowiadać treści SWZ.
3. Ofertę składa się na Formularzu Ofertowym – zgodnie z **Załącznikiem nr 1 do SWZ**. Wraz z ofertą Wykonawca jest zobowiązany złożyć:
   1) oświadczenia, o których mowa w Rozdziale IX ust. 1 SWZ;
   2) zobowiązanie innego podmiotu, o którym mowa w Rozdziale X ust. 3 SWZ (jeżeli dotyczy);
   3) dokumenty, z których wynika prawo do podpisania oferty; odpowiednie pełnomocnictwa (jeżeli dotyczy).
   4) Uzupełniony opz – zgodnie z **Załącznikiem nr 4 do SWZ**
4. Oferta powinna być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy, zgodnie z formą reprezentacji Wykonawcy określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej Wykonawcy albo przez upełnomocnionego przedstawiciela Wykonawcy. W celu potwierdzenia, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania, zamawiający żąda od wykonawcy odpisu lub informacji z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru.
5. Oferta oraz pozostałe oświadczenia i dokumenty, dla których Zamawiający określił wzory w formie formularzy zamieszczonych w załącznikach do SWZ, powinny być sporządzone zgodnie z tymi wzorami, co do treści oraz opisu kolumn i wierszy.
6. **Ofertę składa się pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.**
7. Oferta powinna być sporządzona w języku polskim. Każdy dokument składający się na ofertę powinien być czytelny.
8. Jeśli oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233 z późn. zm..), Wykonawca powinien nie później niż w terminie składania ofert, zastrzec, że nie mogą one być udostępnione oraz wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa..

9. W celu złożenia oferty należy zarejestrować (zalogować) się na Platformie i postępować zgodnie z instrukcjami dostępnymi u dostawcy rozwiązania informatycznego pod adresem ezamowienia.gov.pl
10. Przed upływem terminu składania ofert, Wykonawca może wprowadzić zmiany do złożonej oferty lub wycofać ofertę. W tym celu należy w systemie Platformy kliknąć przycisk „Wycofaj ofertę". Zmiana oferty następuje poprzez wycofanie oferty oraz jej ponownym złożeniu.
11. Podmiotowe środki dowodowe lub inne dokumenty, w tym dokumenty potwierdzające umocowanie do reprezentowania, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
12. Wszystkie koszty związane z uczestnictwem w postępowaniu, w szczególności z przygotowaniem i złożeniem oferty ponosi Wykonawca składający ofertę. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

XIV. SPOSÓB OBLICZENIA CENY OFERTY

1. Wykonawca podaje cenę za realizację przedmiotu zamówienia zgodnie ze wzorem Formularza Ofertowego, stanowiącego **Załącznik nr 1 do SWZ.**
2. Cena ofertowa brutto musi uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia zgodnie z opisem przedmiotu zamówienia oraz istotnymi postanowieniami umowy określonymi w niniejszej SWZ.
3. Cena podana na Formularzu Ofertowym jest ceną ostateczną, niepodlegającą negocjacji i wyczerpującą wszelkie należności Wykonawcy wobec Zamawiającego związane z realizacją przedmiotu zamówienia.
4. Cena oferty powinna być wyrażona w złotych polskich (PLN) z dokładnością do dwóch miejsc po przecinku.
5. Zamawiający nie przewiduje rozliczeń w walucie obcej.
6. Wyliczona cena oferty brutto będzie służyć do porównania złożonych ofert i do rozliczenia w trakcie realizacji zamówienia.
7. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2024 r. poz. 361 z pózn. zm.), dla celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów

i usług, którą miałby obowiązek rozliczyć. W ofercie, o której mowa w ust. 1, wykonawca ma obowiązek:

1) poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego;
2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;
4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

8. Wzór Formularza Ofertowego został opracowany przy założeniu, iż wybór oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego w zakresie podatku VAT. W przypadku, gdy Wykonawca zobowiązany jest złożyć oświadczenie o powstaniu u Zamawiającego obowiązku podatkowego, to winien odpowiednio zmodyfikować treść formularza.
9. Cena ofertowa oraz ceny jednostkowe muszą obejmować wszystkie koszty związane z realizacją przedmiotu zamówienia, w tym wszelkie inne koszty, możliwe upusty i rabaty, a także potencjalne ryzyka ekonomiczne, które mogą wystąpić w trakcie realizacji umowy. Należy również uwzględnić okoliczności, które nie mogły zostać przewidziane w momencie zawierania umowy, w szczególności wszelkie nakłady i prace niezbędne do prawidłowego wykonania przedmiotu zamówienia, bez konieczności ponoszenia przez Zamawiającego jakichkolwiek dodatkowych kosztów.

XV. WYMAGANIA DOTYCZĄCE WADIUM

1. Wykonawca zobowiązany jest do zabezpieczenia swojej oferty wadium w wysokości: **8000,00** (słownie: osiem tysięcy 00/100 złotych);
2. Wadium wnosi się przed upływem terminu składania ofert.
3. Wadium może być wnoszone w jednej lub kilku następujących formach:
   1) pieniądzu;
   2) gwarancjach bankowych;
   3) gwarancjach ubezpieczeniowych;

4) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2020 r. poz. 299).

4. Wadium w formie pieniądza należy wnieść przelewem na konto Zamawiającego nr rachunku 68 9550 0003 2008 0077 0277 0004 z dopiskiem „Wadium – *BSR-ZP.271.3.2026*".

UWAGA: Za termin wniesienia wadium w formie pieniężnej zostanie przyjęty termin uznania rachunku Zamawiającego.

5. Wadium wnoszone w formie poręczeń lub gwarancji musi być złożone jako oryginał gwarancji lub poręczenia w postaci elektronicznej i spełniać co najmniej poniższe wymagania:
   1) musi obejmować odpowiedzialność za wszystkie przypadki powodujące utratę wadium przez Wykonawcę określone w ustawie p.z.p.
   2) z jej treści powinno jednoznacznej wynikać zobowiązanie gwaranta do zapłaty całej kwoty wadium;
   3) powinno być nieodwołalne i bezwarunkowe oraz płatne na pierwsze żądanie;
   4) termin obowiązywania poręczenia lub gwarancji nie może być krótszy niż termin związania ofertą (z zastrzeżeniem iż pierwszym dniem związania ofertą jest dzień składania ofert);
   5) w treści poręczenia lub gwarancji powinna znaleźć się nazwa oraz numer przedmiotowego postępowania;
   6) beneficjentem poręczenia lub gwarancji jest: Gmina Miejska Ciechocinek
   7) w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia (art. 58 p.z.p.), Zamawiający wymaga aby poręczenie lub gwarancja obejmowała swą treścią (tj. zobowiązanych z tytułu poręczenia lub gwarancji) wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia lub aby z jej treści wynikało, że zabezpiecza ofertę Wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum);
6. Oferta wykonawcy, który nie wniesie wadium, wniesie wadium w sposób nieprawidłowy lub nie utrzyma wadium nieprzerwanie do upływu terminu związania ofertą lub złoży wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 p.z.p. zostanie odrzucona.
7. Zasady zwrotu oraz okoliczności zatrzymania wadium określa art. 98 p.z.p.

XVI. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca będzie związany ofertą przez okres 30 dni tj. 26.03.2026 r. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą wskazanego w ust. 1, 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. Przedłużenie terminu związania ofertą wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
3. Odmowa wyrażenia zgody na przedłużenie terminu związania ofertą nie powoduje utraty wadium.

XVII. SPOSÓB I TERMIN SKŁADANIA I OTWARCIA OFERT

1. Ofertę należy złożyć poprzez Platformę do dnia 25.02.2026 r. do godziny 9:00
2. O terminie złożenia oferty decyduje czas pełnego przeprocesowania transakcji na Platformie.
3. Otwarcie ofert nastąpi w dniu 25.02.2026 r. o godzinie 9:15
4. Najpóźniej przed otwarciem ofert, udostępnia się na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza się przeznaczyć na sfinansowanie zamówienia.
5. Niezwłocznie po otwarciu ofert, udostępnia się na stronie internetowej prowadzonego postępowania informacje o:
   1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   2) cenach lub kosztach zawartych w ofertach.

XV. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert:
   1) **Cena (C)** – waga kryterium 60 %;

2) **Gwarancja (G)** – waga kryterium 10%.

3) **Dodatkowa funkcjonalność XDR** – waga 15%

4) **Funkcjonalność SIEM/SOAR** – waga 15%

2. Zasady oceny ofert w poszczególnych kryteriach:

Kryterium ceny zostanie obliczone według poniższego wzoru:

Cena (C) – waga 60%

$$C = \frac{\text{cena najniższa brutto*}}{\text{cena oferty ocenianej brutto}} \text{ x 100 pkt x 60 \%}$$

*** spośród wszystkich złożonych ofert niepodlegających odrzuceniu**

a) Podstawą przyznania punktów w kryterium „cena" będzie cena ofertowa brutto podana przez Wykonawcę w Formularzu Ofertowym.

b) Cena ofertowa brutto musi uwzględniać wszelkie koszty jakie Wykonawca poniesie w związku z realizacją przedmiotu zamówienia.

Kryterium gwarancji

Gwarancja (G) – waga 10 %

Zamawiający w ramach kryterium ,,gwarancja'' będzie przyznawał punkty za zadeklarowanie długości trwania okresu gwarancji przedmiotu zamówienia w następujący sposób:

1) Oferent, który zaoferuje okres gwarancji 24 miesiące– otrzyma 0 pkt
2) Oferent, który zaoferuje okres gwarancji 30 miesięcy - otrzyma 5 pkt
3) Oferent, który zaoferuje okres gwarancji 36 miesięcy – otrzyma 10 pkt

Jeżeli w formularzu ofertowym Wykonawca nie wskaże okresu gwarancji, Zamawiający przyjmie, że Wykonawca zaoferował okres gwarancji wynoszący 24 miesiące i przyzna 0 pkt. w kryterium ,,gwarancja''

Kryterium Dodatkowa funkcjonalność XDR – waga 15%

Zamawiający w ramach kryterium „Dodatkowa funkcjonalność XDR" będzie przyznawał punkty za zadeklarowanie dodatkowej funkcjonalności XDR:

1) Oferent, który zaoferuje rozwiązanie XDR bez możliwości szyfrowania – otrzyma 0 pkt
2) Oferent, który zaoferuje rozwiązanie XDR z możliwością szyfrowania – otrzyma 10 pkt

Jeżeli w formularzu ofertowym Wykonawca nie wskaże, czy oferuje dodatkową funkcjonalność XDR, Zamawiający przyjmie, że Wykonawca zaoferował rozwiązanie XDR bez możliwości szyfrowania i przyzna 0 pkt. w kryterium ,,dodatkowa funkcjonalność XDR''

Kryterium Funkcjonalność SIEM/SOAR – waga 15%

Zamawiający w ramach kryterium **„Funkcjonalność SIEM/SOAR"** będzie przyznawał punkty za zaoferowanie rozwiązania rozszerzającego usługę serwera logów o funkcjonalność systemu klasy SIEM, obejmującą co najmniej korelację zdarzeń, analizę zagrożeń, automatyzację reakcji na incydenty (SOAR) oraz zaawansowane raportowanie bezpieczeństwa.:

1) NIE - 0 pkt
2) TAK - 10 pkt

Jeżeli w formularzu ofertowym Wykonawca nie wskaże, czy oferuje dodatkową funkcjonalność SIEM/SOAR, Zamawiający przyjmie, że Wykonawca zaoferował rozwiązanie bez możliwości rozszerzającej usługę serwera logów o funkcjonalność systemu klasy SIEM, obejmującą co najmniej korelację zdarzeń, analizę zagrożeń, automatyzację reakcji na incydenty (SOAR) oraz zaawansowane raportowanie bezpieczeństwa przyzna 0 pkt. w kryterium ,,dodatkowa funkcjonalność SIEM/SOAR''

3. Punktacja przyznawana ofertom w poszczególnych kryteriach oceny ofert będzie liczona z dokładnością do dwóch miejsc po przecinku, zgodnie z zasadami arytmetyki.

   P = Pc + Pg + Pxdr + Psiem

   P – punkty łącznie

   Pc – punkty w kryterium cena

   Pt – punkty za termin realizacji

   Pxdr – punkty za dodatkową funkcjonalność XDR

   Psiem – punkty za funkcjonalność SIEM/SOAR

4. W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonej oferty, w tym zaoferowanej ceny.
5. Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą.

XVIII. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY BYĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia prowadzonym w trybie podstawowym złożono tylko jedną ofertę.
3. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający zastrzega sobie prawo żądania przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych Wykonawców.
4. Wykonawca będzie zobowiązany do podpisania umowy w miejscu i terminie wskazanym przez Zamawiającego.

XIX. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający **nie wymaga** wniesienia zabezpieczenia należytego wykonania umowy w wysokości 5% wartości zamówienia brutto.

XX. INFORMACJE O TREŚCI ZAWIERANEJ UMOWY ORAZ MOŻLIWOŚCI JEJ ZMIANY

1. Wybrany Wykonawca jest zobowiązany do zawarcia umowy w sprawie zamówienia publicznego na warunkach określonych w Projektowanych Postanowieniach Umownych, stanowiących **Załącznik nr 4 do SWZ**.
2. Zakres świadczenia Wykonawcy wynikający z umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.
3. Zamawiający przewiduje możliwość zmiany zawartej umowy w stosunku do treści wybranej oferty w zakresie uregulowanym w art. 454-455 p.z.p. oraz wskazanym w Projektowanych Postanowieniach Umownych, stanowiące **Załącznik nr 7 do SWZ**.
4. Zmiana umowy wymaga dla swej ważności, pod rygorem nieważności, zachowania formy pisemnej.

XXI. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Środki ochrony prawnej określone w niniejszym dziale przysługują wykonawcy, uczestnikowi konkursu oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy p.z.p.

8. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych, zwanego dalej "sądem zamówień publicznych".
9. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy p.z.p., przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (tekst jedn. 2025 r., poz. 366) jest równoznaczne z jej wniesieniem.
10. Prezes Izby przekazuje skargę wraz z aktami postępowania odwoławczego do sądu zamówień publicznych w terminie 7 dni od dnia jej otrzymania.

XXII. OCHRONA DANYCH OSOBOWYCH

1. Administratorem Pani/Pana danych osobowych jest Skarb Państwa, w imieniu którego działa Centrum Projektów Polska Cyfrowa, z siedzibą w Warszawie, 01-044, przy ul. Spokojnej 13a.
2. W ramach niniejszego postępowania prowadzonego w ramach projektu grantowego „Cyberbezpieczny Samorząd", Zamawiający jest podmiotem przetwarzającym.
3. Klauzula informacyjna Administratora stanowi **załącznik nr 8 do SWZ.**

XXIII. WYKAZ ZAŁĄCZNIKÓW DO SWZ

Załącznik nr 1	Formularz Ofertowy - wzór
Załącznik nr 2	Oświadczenie o braku podstaw do wykluczenia i o spełnianiu warunków udziału w postępowaniu - wzór
Załącznik nr 3	Zobowiązanie innego podmiotu do udostępnienia niezbędnych zasobów Wykonawcy – wzór
Załącznik nr 4	Opis przedmiotu zamówienia
Załącznik nr 5	Wykaz dostaw - wzór
Załącznik nr 6	Projektowane postanowienia umowne – wzór
Załącznik nr 7	Karta gwarancyjna - wzór
Załącznik nr 8	Klauzula informacyjna FERC
Załącznik nr 9	Wykaz osób - wzór

Z up. MINISTRA
mgr Joanna Gryżałowska
Zastępca Ministra

Kierownik
Biura Strategii, Rozwoju
i Zamówień Publicznych
mgr Marcin Graczyk

Specjalista
zamówień publicznych
mgr Ewelina Kurtys-Żak

2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 p.z.p. oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. 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;
4. Odwołanie wnosi się do Prezesa Izby. Odwołujący przekazuje kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
5. Odwołanie wobec treści ogłoszenia lub treści SWZ wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub treści SWZ na stronie internetowej.
6. Odwołanie wnosi się w terminie:
   1) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
   2) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 1).
7. Odwołanie w przypadkach innych niż określone w pkt 5 i 6 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia
6. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy p.z.p., stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
7. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego o apelacji, jeżeli przepisy niniejszego rozdziału nie stanowią inaczej.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 1 do SWZ

.....

(miejsce i data)

Wykonawca:
.....
.....
(nazwa i adres oraz w zależności od podmiotu NIP, KRS/CEiDG)

reprezentowany przez:
.....
.....
(imię, nazwisko, stanowisko/
podstawa do reprezentacji)

Osoba upoważniona do kontaktu z Zamawiającym: ..... tel. .....
e-mail .....

Wykonawca jest: mikro / małym / średnim / dużym przedsiębiorcą*

*niepotrzebne skreślić

1. Odpowiadając na publiczne ogłoszenie o zamówieniu w postępowaniu nr BSR-ZP.271.3.2026 pn.,, Dostawa sprzętu i oprogramowania dla Gminy Miejskiej Ciechocinek" składamy następującą ofertę:

Oferujemy realizację przedmiotu zamówienia – zgodnie z warunkami i na zasadach zawartych w SWZ za wynagrodzeniem w wysokości:
..... zł brutto (słownie:..... 00/100),
w tym wartość netto ..... + VAT .....

Wskazana kwota została obliczona z sumowania wartości wynikającej z poniższej Tabeli.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 1 do SWZ

Tabela

	Przedmiot oferty		Cena jednostkowa brutto	Ilość	Wartość łączna brutto
Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ I	Nazwa producenta			3	
	Model lub symbol jednoznacznie określający urządzenie:				
Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ II	Nazwa producenta:			5	
	Model lub symbol jednoznacznie określający urządzenie:				
Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ I	Nazwa producenta serwera:			1	
	Model lub symbol jednoznacznie określający urządzenie:				
	Model procesora:				
	Nazwa i wersja systemu operacyjnego:				
	Nazwa producenta serwera:			5	

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 1 do SWZ

Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ II	Model lub symbol jednoznacznie określający urządzenie:				
	Model procesora:				
	Nazwa i wersja systemu operacyjnego:				
Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ III	Nazwa producenta serwera:			1	
	Model lub symbol jednoznacznie określający urządzenie:				
	Model procesora:				
	Nazwa i wersja systemu operacyjnego:				
Wdrożenie usługi serwera logów systemowych i stacji końcowych oraz sieciowych	Nazwa producenta:			7	
	Nazwa oprogramowania:				
	Wersja oprogramowania/nazwa modułów/pakietów licencji (wpisać dane wskazujące oferowane oprogramowanie)				
	Nazwa producenta:			7	

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 1 do SWZ

Urządzenie typu NAS na potrzeby kopii wraz z instalacją i konfiguracją	Model lub symbol jednoznacznie określający urządzenie:				
Backupowy serwer redundancji usług	Nazwa producenta serwera:			1	
	Model lub symbol jednoznacznie określający urządzenie:				
	Model procesora:				
	Nazwa i wersja systemu operacyjnego:				
Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (Ośrodek Sportu i Rekreacji w Ciechocinku)	**System SAM**			1	
	Nazwa producenta:				
	Nazwa oprogramowania:				
Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (Miejski	Wersja oprogramowania/nazwa modułów/pakietów licencji (wpisać dane wskazujące oferowane oprogramowanie)			1	

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 1 do SWZ

Ośrodek Pomocy Społecznej)				
Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (Szkoła Podstawowa nr 1)			1	
Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (Szkoła Podstawowa nr 3)			1	
Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (Przedszkole Samorządowe nr 1, Przedszkole Samorządowe nr 2,			3	

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 1 do SWZ

Żłobek Samorządowy „Bajeczka")				
Wdrożenie rozwiązań XDR i SIEM do monitoringu stacji końcowych (**Urząd Miasta w Ciechocinku**)	**System XDR**	XDR: .....zł SIEM: .....zł	**1**	
	Nazwa producenta:			
	Nazwa oprogramowania:			
	Wersja oprogramowania/nazwa modułów/pakietów licencji (wpisać dane wskazujące oferowane oprogramowanie)			
	Czy zaoferowany system XDR posiada funkcjonalność szyfrowania?	TAK/NIE (wybrać właściwe)		
Wdrożenie rozwiązań XDR i SIEM do monitoringu stacji końcowych (**Ośrodek Sportu i Rekreacji**)		XDR: .....zł SIEM: .....zł	**1**	
Wdrożenie rozwiązań XDR i SIEM do monitoringu stacji końcowych (**Miejski Ośrodek Pomocy Społecznej**)		XDR: .....zł SIEM: .....zł	**1**	
Wdrożenie rozwiązań XDR i SIEM do monitoringu stacji końcowych (**Szkoła Podstawowa nr 1**)		XDR: .....zł SIEM: .....zł	**1**	

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 1 do SWZ

Wdrożenie rozwiązań XDR i SIEM do monitoringu stacji końcowych (**Szkoła Podstawowa nr 3**)	**System SIEM**		XDR: .....zł SIEM: .....zł	**1**	
	Nazwa producenta:				
	Nazwa oprogramowania:				
	Wersja oprogramowania/nazwa modułów/pakietów licencji (wpisać dane wskazujące oferowane oprogramowanie)				
	Zaoferowane rozwiązanie stanowi rozbudowę „usługi serwera logów systemowych i stacji końcowych oraz sieciowych" opisanej w poz. III OPZ, poprzez jej rozszerzenie o funkcjonalności systemu klasy SIEM, w szczególności w zakresie korelacji zdarzeń, analizy zagrożeń, automatyzacji reakcji na incydenty (SOAR) oraz rozszerzonego raportowania bezpieczeństwa.	TAK/NIE (wybrać właściwe)			
Wdrożenie rozwiązań XDR i SIEM do monitoringu stacji końcowych (**Przedszkole Samorządowe nr 1**)			XDR: .....zł SIEM: .....zł	**1**	
Wdrożenie rozwiązań XDR i SIEM do monitoringu stacji końcowych (**Przedszkole Samorządowe nr 2**)			XDR: .....zł SIEM: .....zł	**1**	
Wdrożenie rozwiązań XDR i SIEM do monitoringu stacji końcowych (**Żłobek Samorządowy „Bajeczka"**)			XDR: .....zł SIEM: .....zł	**1**	

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 1 do SWZ

2. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.
3. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku (uzupełnić wskazane informacje, jeżeli dotyczy)
   .....
4. Oświadczamy, iż zaoferowana (-e) cena (-y) podana (-e) w ofercie zawiera (-ją) wszelkie koszty poniesione w celu należytego wykonania zamówienia zgodnie z wymaganiami Zamawiającego zawartymi w SWZ i wszystkich załącznikach do niej jak również w niej nie ujęte, a bez których nie można wykonać zamówienia, a także wszelkie podatki (także należny podatek VAT). Cena obejmuje ewentualne marże i opusty.
5. Jednocześnie oświadczam, że:

1) Zobowiązujemy się zrealizować przedmiot zamówienia w terminie wskazanym w Specyfikacji Warunków Zamówienia.
2) Akceptujemy warunki płatności podane we wzorze umowy.
3) Warunki udziału w postępowaniu spełniamy samodzielnie/ polegamy na zasobach podmiotu trzeciego*

*niepotrzebne skreślić

4) Podwykonawcy/om
   tj.....
   (nazwa podwykonawcy)

   powierzymy następującą część/części zamówienia, (jeżeli dotyczy)
   :.....
5) Zobowiązujemy się skierować do wykonania przedmiotu zamówienia wykwalifikowany personel dysponujący odpowiednią wiedzą oraz uprawnieniami.
6) Na koordynatora realizacji przedmiotu zamówienia wyznaczamy p.
   ....., tel.:..... e-mail:.....
7) Oświadczamy, iż zapoznaliśmy się ze Specyfikacją Warunków Zamówienia, nie wnosimy do niej zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty i zobowiązujemy się spełnić wszystkie wymagania Zamawiającego, wymienione w SWZ i we wszystkich załącznikach do niej.
8) Jesteśmy związani niniejszą ofertą przez czas wskazany w Specyfikacji Warunków Zamówienia.
9) Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 1 do SWZ

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 119 z 04.05.2016, str. 1), dalej „RODO", wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

10) Zawarta w Specyfikacji Warunków Zamówienia treść wzoru umowy została przez nas zaakceptowana i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na wyżej wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.

11) Dokumenty wymagane w SWZ, jakie Zamawiający może uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne:

.....

12) Zgodnie z SWZ wskazujemy, że tajemnicą przedsiębiorstwa objęte są następujące elementy oferty:

.....

13) Znając treść przepisu art. 297 §1 Kodeksu Karnego:
„Kto, w celu uzyskania dla siebie lub kogo innego, od banku lub jednostki organizacyjnej prowadzącej podobną działalność gospodarczą na podstawie ustawy albo od organu lub instytucji dysponujących środkami publicznymi – kredytu, pożyczki pieniężnej, poręczenia, gwarancji, akredytywy, dotacji, subwencji, potwierdzenia przez bank zobowiązania wynikającego z poręczenia lub z gwarancji lub podobnego świadczenia pieniężnego na określony cel gospodarczy, instrumentu płatniczego lub zamówienia publicznego, przedkłada podrobiony, przerobiony, poświadczający nieprawdę albo nierzetelny dokument albo nierzetelne, pisemne oświadczenie dotyczące okoliczności o istotnym znaczeniu dla uzyskania wymienionego wsparcia finansowego, instrumentu płatniczego lub zamówienia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5", oświadczamy, że dane zawarte w ofercie, dokumentach i oświadczeniach są zgodne ze stanem faktycznym.

14) Wraz z niniejszą ofertą składamy:

Nazwa załącznika

1) .....

2) .....

Dokument należy opatrzyć
kwalifikowanym podpisem elektronicznym
lub podpisem zaufanym
albo podpisem osobistym

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 2 do SWZ

.....
(miejscowość, data)

Wykonawca:
.....
.....
(nazwa i adres oraz w zależności od podmiotu NIP, KRS/CEiDG)

reprezentowany przez:
.....
.....
(imię, nazwisko, stanowisko/
podstawa do reprezentacji)

Oświadczenie Wykonawcy
o niepodleganiu wykluczeniu i spełnieniu warunków udziału w postępowaniu
składane na podstawie art. 125 ust. 1 w zw. z art. 266 ustawy z 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320 z późn. zm.), dalej: „ustawa Pzp"

Na potrzeby postępowania o udzielenie zamówienia publicznego nr BSR-ZP.271.3.2026 pn.: ,,Dostawa sprzętu i oprogramowania dla Gminy Miejskiej Ciechocinek" oświadczam, co następuje:

I. Oświadczenie dotyczące Wykonawcy:

1. Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w Specyfikacji Warunków Zatrudnienia.
2. Oświadczam, iż nie podlegam wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 108 ust 1 ustawy Pzp,
3. Oświadczam, iż nie podlegam wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 109 ust. 1 ustawy Pzp,
4. W związku z art. 7 ust. 1 ustawy z 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego oświadczam, że wykonawca:

1) jest*/nie jest* wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ww. ustawy;
2) jest*/nie jest* beneficjentem rzeczywistym wykonawcy w rozumieniu ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tekst jedn.: Dz.U. z 2022 r. poz. 593 ze zm.),
3) jest*/nie jest* osobą wymienioną w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisaną na listę lub będącą takim beneficjentem rzeczywistym od 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 ww. ustawy;
4) jest*/nie jest* jednostką dominującą wykonawcy w rozumieniu art. 3 ust. 1 pkt 37 ustawy z 29 września 1994 r. o rachunkowości (tekst jedn.: Dz.U. z 2021 r. poz. 217 ze zm.),
5) jest*/nie jest* podmiotem wymienionym w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanym na listę lub będącym taką jednostką dominującą od 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 ww. ustawy.

5. W związku z art. 5k ust. 1 Rozporządzenia Rady (UE) Nr 833/2014 z 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie oświadczam, że:
   1) jestem* / nie jestem* obywatelem rosyjskim lub osobą fizyczną lub prawną, podmiotem lub organem z siedzibą w Rosji,
   2) jestem* / nie jestem* osobą prawną, podmiotem lub organem, do których prawa własności bezpośrednio lub pośrednio w ponad 50% należą do podmiotu, którego prawa własnościowe są bezpośrednio lub pośrednio w ponad 50% własnością osoby fizycznej lub prawnej, jednostki lub organu, o których mowa w pkt 1,
   3)jestem* / nie jestem* osobą fizyczną lub prawną, podmiotem lub organem działającym w imieniu lub pod kierunkiem podmiotu, o którym mowa w pkt 1 lub 2;
6. W związku z art. 5k ust. 1 Rozporządzenia Rady (UE) Nr 833/2014 z 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie zobowiązujemy się nie wykonywać zamówienia z udziałem podwykonawców, dostawców lub podmiotów, na których zdolności polega się w rozumieniu dyrektywy 2014/24/UE, o których mowa w art. 5k rozporządzenia Rady (UE) nr 833/2014 z 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie, w przypadku gdy przypada na nich ponad 10% wartości zamówienia.

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 2 do SWZ

II. Self – cleaning (jeżeli dotyczy)

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ..... ustawy Pzp*. Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:
.....
.....

III. Oświadczenie dotyczące podmiotu, na którego zasoby powołuje się Wykonawca:

Oświadczam, że następujący/e podmiot/y, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.: .....* nie podlega/ją wykluczeniu z postępowania o udzielenie zamówienia.

(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

IV. 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.

Dokument należy opatrzyć
kwalifikowanym podpisem elektronicznym
lub podpisem zaufanym
albo podpisem osobistym

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 3 do SWZ

.....

(miejscowość i data)

Podmiot udostępniający zasoby:

.....

.....

(nazwa i adres)

ZOBOWIĄZANIE PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY

Zobowiązuję się do oddania Wykonawcy - .....

(podać nazwę i adres) do dyspozycji następujących niezbędnych zasobów na potrzeby realizacji zamówienia pn. ,, Dostawa sprzętu i oprogramowania dla Gminy Miejskiej Ciechocinek'', w zakresie warunku/warunków udziału w postępowaniu, tj.

.....

Oświadczam, że stosunek łączący mnie z ww. Wykonawcą gwarantuje rzeczywisty dostęp do udostępnianych mu zasobów, na potwierdzenie czego przedstawiam, co następuje:

1. zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby:

   .....

2. sposób i okres udostępniania Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia:

   .....

3. informację, 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/usługi, których wskazane zdolności dotyczą:

   .....

Spis treści

Postanowienia ogólne – wymagania wstępne

1. Niniejszy Opis Przedmiotu Zamówienia (OPZ) określa minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia, których spełnienie jest obowiązkowe dla Wykonawcy.
2. Wykonawca zobowiązany jest wykazać, że oferowany przedmiot zamówienia jest w pełni zgodny z wymaganiami określonymi w niniejszym OPZ.
3. Niespełnienie któregokolwiek z wymagań określonych w OPZ skutkować będzie odrzuceniem oferty jako niezgodnej z SWZ, zgodnie z obowiązującymi przepisami prawa.
4. Złożenie oferty w niniejszym postępowaniu oznacza, że Wykonawca potwierdza spełnienie wszystkich poniżej określonych wymagań oraz oferuje przedmiot zamówienia zgodny z niniejszym OPZ, w szczególności, że:

   a) dostarczane urządzenia oraz oprogramowanie będą fabrycznie nowe, nieużywane, nieuszkodzone, wolne od wad prawnych i fizycznych, nieobciążone prawami osób trzecich, pochodzące z bieżącej oferty producenta oraz niebędące w fazie wycofania z produkcji (EOL) na dzień złożenia oferty;

b) dostarczony sprzęt oraz oprogramowanie będą pochodzić z oficjalnych kanałów dystrybucyjnych producenta, obejmujących rynek Unii Europejskiej, zapewniających realizację uprawnień gwarancyjnych oraz dostęp do wsparcia technicznego i części zamiennych; Zamawiający zastrzega, że urządzenia i ich podzespoły nie muszą być wyprodukowane na terenie Unii Europejskiej, jednak muszą być dopuszczone do obrotu na terenie UE oraz spełniać obowiązujące normy i przepisy;
wszystkie urządzenia muszą posiadać oznakowanie CE oraz być przystosowane do pracy w sieci energetycznej o parametrach 230 V ±10%, 50 Hz;

c) całość dostarczanego rozwiązania, tj. każde z dostarczonych urządzeń, dla którego nie wskazano odmiennych warunków gwarancyjnych w OPZ, objęta będzie minimum 24-miesięczną gwarancją producenta;

d) Wykonawca zapewni odpowiednie opakowanie i zabezpieczenie sprzętu na czas transportu, gwarantujące brak uszkodzeń lub pogorszenia jakości do momentu dostarczenia do miejsca wskazanego przez Zamawiającego;

e) do każdego urządzenia oraz oprogramowania dostarczony zostanie komplet niezbędnych akcesoriów eksploatacyjnych (w szczególności przewody zasilające, sygnałowe i inne elementy konieczne do uruchomienia), stanowiących integralną część oferty i przechodzących na własność Zamawiającego;

f) do każdego urządzenia oraz oprogramowania dostarczona zostanie standardowa dokumentacja użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim; w przypadku dokumentacji udostępnianej wyłącznie w formie elektronicznej Wykonawca przekaże Zamawiającemu adresy stron internetowych, z których możliwe jest jej pobranie.

5. Wykonawca zobowiązany jest do dostarczenia, instalacji, konfiguracji oraz wdrożenia urządzeń i oprogramowania do pracy w ramach infrastruktury teleinformatycznej Zamawiającego, w tym do wykonania niezbędnych połączeń technicznych i logicznych oraz konfiguracji ustawień zapewniających prawidłowe i bezpieczne działanie systemów, zgodnie z wymaganiami OPZ oraz wytycznymi administratorów Zamawiającego.

6. W zakresie oprogramowania Wykonawca zobowiązany jest do zapewnienia Zamawiającemu prawa do korzystania z oprogramowania w formie niewyłącznej licencji lub innego równoważnego uprawnienia licencyjnego, zgodnie z zasadami licencjonowania określonymi przez producenta.

7. Oprogramowanie dostarczone w ramach zamówienia musi być dostarczone w najnowszej stabilnej wersji dostępnej na dzień dostawy, posiadającej wsparcie producenta oraz – jeżeli dotyczy – certyfikację producenta sprzętu, z którym ma współpracować.

Część A. Opis techniczny

I.1. Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ I – 3 szt.

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.	
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.	
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 5 portami Gigabit Ethernet RJ-45. • System Firewall posiada wbudowany port konsoli szeregowej. 2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.	
Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 500 tys. jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 1,3 Gbps.	

	5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 600 Mbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 400 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 250 Mbps.	
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).	
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.	

	5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z **co najmniej trzema** popularnymi platformami chmurowymi / SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu, w tym przykładowo: • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.	
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.	
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego.	

	2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.	
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi	

	serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.	
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.	
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).	

Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.	
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.	

	2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.	
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.	
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.	
Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w	

	przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.	
Wdrożenie	1. Konfiguracja dostarczonego sprzętu i oprogramowania: - aktualizacja do najnowszej zalecanej wersji oprogramowania - konfiguracja interfejsów - konfiguracja routingu - konfiguracja VPN - stworzenie segmentów sieci - stworzenie profili bezpieczeństwa takich jak AV, kontrola treści, kontrola aplikacji, IPS - stworzenie obiektów - stworzenie przykładowych polityk zezwalających na ruch pomiędzy segmentami 2. Przeniesienie bram lub stworzenie bram na dostarczonym urządzeniu.	
Inne	Zaleca się, aby w przypadku istnienia wymogów prawnych odnoszących się do technologii objętej przedmiotem niniejszego postępowania, w szczególności w zakresie tzw. produktów podwójnego zastosowania, Wykonawca posiadał lub był w stanie przedstawić na żądanie Zamawiającego dokument pochodzący od importera danej technologii, potwierdzający, że przy jej wprowadzeniu na terytorium Rzeczypospolitej Polskiej zostały dochowane wymogi właściwych przepisów prawa, w tym przepisów dotyczących obrotu z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa oraz dla utrzymania międzynarodowego pokoju i bezpieczeństwa, a także dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę wewnętrzny system kontroli, wymagany w ramach wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Zaleca się, aby Wykonawca posiadał lub był w stanie przedstawić na żądanie Zamawiającego dokument w postaci oświadczenia producenta lub autoryzowanego dystrybutora producenta na terytorium Rzeczypospolitej Polskiej, potwierdzający, że oferowany produkt pochodzi z autoryzowanego kanału sprzedaży, w szczególności poprzez wykazanie posiadanego statusu autoryzacyjnego lub innego równoważnego potwierdzenia.	

I.2. Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ II – 4 szt.

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
Wymagania Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od	

	dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.	
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.	
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.	
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6.2 Gbps.	

	5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 620 Mbps.	
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL.	
Polityki, Firewall	3. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 4. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 5. Translację jeden do jeden oraz jeden do wielu. 6. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 7. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 8. Element systemu realizujący funkcję Firewall integruje się z **co najmniej trzema** popularnymi platformami chmurowymi / SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu, w tym przykładowo: 9. Amazon Web Services (AWS). 10. Microsoft Azure 11. Cisco ACI. 12. Google Cloud Platform (GCP).	

	13. OpenStack. VMware vCenter (ESXi).	
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.	
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.	

	System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.	

	5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	

	7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.	
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesiące.	
Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesiące, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	
Wdrożenie	1. Konfiguracja dostarczonego sprzętu i oprogramowania: - aktualizacja do najnowszej zalecanej wersji oprogramowania - konfiguracja interfejsów - konfiguracja routingu - konfiguracja VPN - stworzenie segmentów sieci - stworzenie profili bezpieczeństwa takich jak AV,kontrola treści, kontrola aplikacji, IPS - stworzenie obiektów - stworzenie przykładowych polityk zezwalających na ruch pomiędzy segmentami 2. Przeniesienie bram lub stworzenie bram na dostarczonym urządzeniu.	

Inne	Zaleca się, aby w przypadku istnienia wymogów prawnych odnoszących się do technologii objętej przedmiotem niniejszego postępowania, w szczególności w zakresie tzw. produktów podwójnego zastosowania, Wykonawca posiadał lub był w stanie przedstawić na żądanie Zamawiającego dokument pochodzący od importera danej technologii, potwierdzający, że przy jej wprowadzeniu na terytorium Rzeczypospolitej Polskiej zostały dochowane wymogi właściwych przepisów prawa, w tym przepisów dotyczących obrotu z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa oraz dla utrzymania międzynarodowego pokoju i bezpieczeństwa, a także dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę wewnętrzny system kontroli, wymagany w ramach wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Zaleca się, aby Wykonawca posiadał lub był w stanie przedstawić na żądanie Zamawiającego dokument w postaci oświadczenia producenta lub autoryzowanego dystrybutora producenta na terytorium Rzeczypospolitej Polskiej, potwierdzający, że oferowany produkt pochodzi z autoryzowanego kanału sprzedaży, w szczególności poprzez wykazanie posiadanego statusu autoryzacyjnego lub innego równoważnego potwierdzenia.	

II.1. Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ I – 1 szt.

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
Obudowa	Obudowa typu Tower z możliwością instalacji 3 dysków twardych 3,5"i dwóch dysków 2.5"	
Płyta główna	Z możliwością instalacji jednego procesora, posiadająca minimum 4 sloty na pamięć RAM UDIMM z możliwością zainstalowania do minimum 128GB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna dedykowana do oferowanego serwera, przystosowana do pracy ciągłej 24/7, objęta wsparciem producenta serwera w okresie gwarancji	
Procesor	Zainstalowany procesor min. 6-rdzeniowy klasy x86, 3.1GHz częstotliwości bazowej, dedykowany do pracy z zaoferowanym serwerem, posiadający funkcjonalność Hyper Threading, umożliwiający osiągnięcie wyniku min. 70 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej (lub równoważnym, opublikowanym przez niezależną organizację branżową, dla konfiguracji jednoprocesorowej). **(na potwierdzenie do oferty należy załączyć wydruk ze strony dla oferowanego procesora).**	
Pamięć RAM	64 GB pamięci RAM ECC o częstotliwości taktowania minimum 5600 MHz, typu UDIMM lub równoważnej. Zgodne z technologią ECC.	
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum 1 slot PCI Express x8 Gen4	

	- minimum 1 slot PCI Express x16 Gen4	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)	
Dyski twarde	Możliwość instalacji dysków twardych 3,5 i 2,5 " typu: SATA, SAS, SSD. Zainstalowane 2 dyski SSD SATA o pojemności min. 1,92TB, RI. Możliwość zainstalowania karty obsługującej dyski samoszyfrujące M.2 NVMe o pojemności min. 960GB z możliwością konfiguracji RAID 1.	
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10	
Wbudowane porty	Minimum 8 portów USB na zewnątrz obudowy z czego min. 4 w technologii 3.x. Minimum 1 port VGA. Minimum 1 port RS-232.	
Video	Zintegrowana karta graficzna.	
Chłodzenie i zasilanie	Zasilacz o mocy minimum 500W. Kable zasilające: 2x C13/C14 10A 2x Kabel z wtyczką europejską	
System operacyjny	Windows Server 2025 Standard lub równoważny serwerowy system operacyjny, spełniający wymagania funkcjonalne opisane poniżej: Licencja na serwerowy system operacyjny, w wersji najnowszej oferowanej przez producenta musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zaoferowanym serwerze. Licencja systemu operacyjnego musi być zgodna z zasadami licencjonowania producenta i umożliwiać legalne korzystanie z usług serwera przez minimum **70 użytkowników,** przy czym wymagane licencje dostępowe (CAL lub równoważne) muszą być zapewnione zgodnie z tymi zasadami. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 2) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 3) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 4) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten	

	musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 5) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 6) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 7) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 8) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 9) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 10) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 11) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 12) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 13) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 14) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 15) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,	

	II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: I. Dystrybucję certyfikatów poprzez http II. Konsolidację CA dla wielu lasów domeny, III. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, IV. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. III. Obsługi 4-KB sektorów dysków IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra V. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. VI. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 16) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 17) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.	

	Za system równoważny uznaje się system operacyjny, który zapewnia wszystkie wymagane funkcjonalności w sposób natywny lub przy użyciu wbudowanych mechanizmów producenta, bez konieczności zakupu dodatkowych licencji innych producentów.	
Diagnostyka i Bezpieczeństwo	• zintegrowany z płytą główną moduł TPM 2.0 • Możliwość wyłączenia w BIOS funkcji przycisku zasilania.	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera	
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą: ○ ISO-9001:2015 **(certyfikat załączyć do oferty)** ○ ISO-14001 **(certyfikat załączyć do oferty)** • Serwer musi posiadać deklaracja CE **(załączyć do oferty)** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Server 2022 lub Microsoft Windows Server 2025. **(na potwierdzenie do oferty należy załączyć wydruk ze strony).**	
Warunki gwarancji	24 miesiące gwarancji, realizowanej w miejscu instalacji urządzenia (on-site), z czasem reakcji serwisowej nie dłuższym niż następny dzień roboczy od momentu przyjęcia zgłoszenia. Zgłaszanie awarii musi być możliwe w trybie 24x7x365, za pośrednictwem ogólnodostępnego kanału zgłoszeniowego (telefonicznego lub elektronicznego). W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Serwis gwarancyjny może być realizowany przez producenta urządzenia, autoryzowanego partnera serwisowego producenta lub inny podmiot posiadający równoważny system serwisowy, zapewniający spełnienie wymaganych warunków gwarancji oraz poziomu SLA określonego w niniejszym opisie.	

	Podmiot realizujący serwis powinien posiadać certyfikat ISO 9001:2015 lub równoważny. (**Dokumenty potwierdzające spełnienie wymagań należy dołączyć do oferty.**) W przypadku zaoferowania certyfikatu równoważnego lub innych środków potwierdzających stosowanie równoważnego systemu zarządzania jakością, Wykonawca zobowiązany jest wykazać równoważność poprzez przedstawienie dokumentów potwierdzających, że stosowany system zapewnia poziom zarządzania jakością nie gorszy niż wymagany w normie ISO 9001:2015, w szczególności w zakresie świadczenia usług serwisowych. Wykonawca zobowiązany jest zapewnić możliwość sprawdzenia statusu gwarancji urządzenia przy użyciu unikatowego numeru identyfikacyjnego oraz dostęp do uaktualnień mikrokodu i sterowników producenta, co najmniej w okresie obowiązywania gwarancji.	
Wdrożenie	• Instalacja serwera w miejscu wskazanym przez Zamawiającego • Podłączenie serwerów do zasilania, sieci LAN • Konfiguracja kart zarządzających (IP, powiadomienia email) • Konfiguracja systemu operacyjnego na serwerach • Przygotowanie dokumentacji powdrożeniowej	

II.2. Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ II – 5 szt.

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
Obudowa	Obudowa typu Tower z możliwością instalacji 3 dysków twardych 3,5"i dwóch 2.5"	
Płyta główna	Z możliwością instalacji jednego procesora, posiadająca minimum 4 sloty na pamięć RAM UDIMM z możliwością zainstalowania do minimum 128GB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna dedykowana do oferowanego serwera, przystosowana do pracy ciągłej 24/7, objęta wsparciem producenta serwera w okresie gwarancji	
Procesor	Zainstalowany procesor min. 6-rdzeniowy klasy x86, 3.1GHz częstotliwości bazowej, dedykowany do pracy z zaoferowanym serwerem, posiadający funkcjonalność Hyper Threading, umożliwiający osiągnięcie wyniku min. 70 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej. (lub równoważnym, opublikowanym przez niezależną organizację branżową, dla konfiguracji jednoprocesorowej). **(na potwierdzenie do oferty należy załączyć wydruk ze strony dla oferowanego procesora).**	

Pamięć RAM	64 GB pamięci RAM ECC o częstotliwości taktowania minimum 5600 MHz, typu UDIMM lub równoważnej. Zgodne z technologią ECC.	
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum 1 slot PCI Express x8 Gen4 - minimum 1 slot PCI Express x16 Gen4	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)	
Dyski twarde	Możliwość instalacji dysków twardych 3,5 i 2,5 ” typu: SATA, SAS, SSD. Zainstalowane: • 2 dyski SSD SATA o pojemności min. 1,92TB, RI. Możliwość zainstalowania karty obsługującej dyski samoszyfrujące M.2 NVMe o pojemności min. 960GB z możliwością konfiguracji RAID 1.	
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10,.	
Wbudowane porty	Minimum 8 portów USB na zewnątrz obudowy z czego min. 4 w technologii 3.x. Minimum 1 port VGA. Minimum 1 port RS-232.	
Video	Zintegrowana karta graficzna.	
Chłodzenie i zasilanie	Zasilacz o mocy minimum 500W. Kable zasilające: 2x C13/C14 10A 2x Kabel z wtyczką europejską	
System operacyjny	Windows Server 2025 Essentials lub równoważny serwerowy system operacyjny, spełniający wymagania funkcjonalne opisane poniżej: Licencja na serwerowy system operacyjny w wersji najnowszej oferowanej przez producenta, umożliwiająca instalację systemu w środowisku fizycznym lub w środowisku wirtualnym, zgodnie z zasadami licencjonowania producenta.Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zaoferowanym serwerze. Licencja systemu operacyjnego musi być zgodna z zasadami licencjonowania producenta i umożliwiać legalne korzystanie z usług serwera przez minimum **25 użytkowników,** przy czym wymagane licencje dostępowe (CAL lub równoważne) muszą być zapewnione zgodnie z tymi zasadami. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość uruchamiania oraz zarządzania maszynami wirtualnymi w obrębie jednego serwera fizycznego. 2) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 3) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 4) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten	

	musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 5) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 6) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 7) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 8) Możliwość obsługi i dystrybucji ruchu sieciowego HTTP w ramach usług serwera WWW 9) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 10) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 11) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 12) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 13) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 14) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 15) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,	

	III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA) umożliwiające podstawowe usługi infrastruktury klucza publicznego (PKI), w tym wystawianie i dystrybucję certyfikatów X.509 w obrębie środowiska. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Możliwość zapewnienia ciągłości pracy usług na poziomie pojedynczego serwera 16) Możliwość automatycznej aktualizacji systemu w oparciu o poprawki publikowane przez producenta oraz zarządzania aktualizacjami przy użyciu bezpłatnych narzędzi producenta. 17) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. *Za system równoważny uznaje się system operacyjny, który zapewnia wszystkie wymagane funkcjonalności w sposób natywny lub przy użyciu wbudowanych mechanizmów producenta, bez konieczności zakupu dodatkowych licencji innych producentów.*	
Diagnostyka i Bezpieczeństwo	• zintegrowany z płytą główną moduł TPM 2.0 • Możliwość wyłączenia w BIOS funkcji przycisku zasilania.	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera	
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą: ○ ISO-9001:2015 **(certyfikat załączyć do oferty)** ○ ISO-14001 **(certyfikat załączyć do oferty)** • Serwer musi posiadać deklaracja CE **(załączyć do oferty)**	

	Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Server 2022 lub Microsoft Windows Server 2025. **(na potwierdzenie do oferty należy załączyć wydruk ze strony).**	
Warunki gwarancji	24 miesiące gwarancji, realizowanej w miejscu instalacji urządzenia (on-site), z czasem reakcji serwisowej nie dłuższym niż następny dzień roboczy od momentu przyjęcia zgłoszenia. Zgłaszanie awarii musi być możliwe w trybie 24x7x365, za pośrednictwem ogólnodostępnego kanału zgłoszeniowego (telefonicznego lub elektronicznego). W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Serwis gwarancyjny może być realizowany przez producenta urządzenia, autoryzowanego partnera serwisowego producenta lub inny podmiot posiadający równoważny system serwisowy, zapewniający spełnienie wymaganych warunków gwarancji oraz poziomu SLA określonego w niniejszym opisie. Podmiot realizujący serwis powinien posiadać certyfikat ISO 9001:2015 lub równoważny. (**Dokumenty potwierdzające spełnienie wymagań należy dołączyć do oferty.**) W przypadku zaoferowania certyfikatu równoważnego lub innych środków potwierdzających stosowanie równoważnego systemu zarządzania jakością, Wykonawca zobowiązany jest wykazać równoważność poprzez przedstawienie dokumentów potwierdzających, że stosowany system zapewnia poziom zarządzania jakością nie gorszy niż wymagany w normie ISO 9001:2015, w szczególności w zakresie świadczenia usług serwisowych. Wykonawca zobowiązany jest zapewnić możliwość sprawdzenia statusu gwarancji urządzenia przy użyciu unikatowego numeru identyfikacyjnego oraz dostęp do uaktualnień mikrokodu i sterowników producenta, co najmniej w okresie obowiązywania gwarancji.	
Wdrożenie	• Instalacja serwera w miejscu wskazanym przez Zamawiającego • Podłączenie serwerów do zasilania, sieci LAN • Konfiguracja kart zarządzających (IP, powiadomienia email) • Konfiguracja systemu operacyjnego na serwerach • Przygotowanie dokumentacji powdrożeniowej	

II.3. Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ III – 1 szt.

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE

Obudowa	Obudowa typu Tower z możliwością instalacji 3 dysków twardych 3,5"i dwóch 2.5"	
Płyta główna	Z możliwością instalacji jednego procesora, posiadająca minimum 4 sloty na pamięć RAM UDIMM z możliwością zainstalowania do minimum 128GB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna dedykowana do oferowanego serwera, przystosowana do pracy ciągłej 24/7, objęta wsparciem producenta serwera w okresie gwarancji	
Procesor	Zainstalowany procesor min. 6-rdzeniowy klasy x86, 3.1GHz częstotliwości bazowej, dedykowany do pracy z zaoferowanym serwerem, posiadający funkcjonalność Hyper Threading, umożliwiający osiągnięcie wyniku min. 70 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej. (lub równoważnym, opublikowanym przez niezależną organizację branżową, dla konfiguracji jednoprocesorowej). **(na potwierdzenie do oferty należy załączyć wydruk ze strony dla oferowanego procesora).**	
Pamięć RAM	64 GB pamięci RAM ECC o częstotliwości taktowania minimum 5600 MHz, typu UDIMM lub równoważnej. Zgodne z technologią ECC.	
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum 1 slot PCI Express x8 Gen4 - minimum 1 slot PCI Express x16 Gen4	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)	
Dyski twarde	Możliwość instalacji dysków twardych 3,5 i 2,5 " typu: SATA, SAS, SSD. Zainstalowane: • 2 dyski SSD SATA o pojemności min. 1,92TB, RI. Możliwość zainstalowania karty obsługującej dyski samoszyfrujące M.2 NVMe o pojemności min. 960GB z możliwością konfiguracji RAID 1.	
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10,.	
Wbudowane porty	Minimum 8 portów USB na zewnątrz obudowy z czego min. 4 w technologii 3.x. Minimum 1 port VGA. Minimum 1 port RS-232.	
Video	Zintegrowana karta graficzna.	
Chłodzenie i zasilanie	Zasilacz o mocy minimum 500W. Kable zasilające: 2x C13/C14 10A 2x Kabel z wtyczką europejską	
System operacyjny	Windows Server 2025 Standard lub równoważny serwerowy system operacyjny, spełniający wymagania funkcjonalne opisane poniżej: Licencja na serwerowy system operacyjny, w wersji najnowszej oferowanej przez producenta musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego.	

	Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zaoferowanym serwerze. Licencja systemu operacyjnego musi być zgodna z zasadami licencjonowania producenta i umożliwiać legalne korzystanie z usług serwera przez minimum **40 użytkowników,** przy czym wymagane licencje dostępowe (CAL lub równoważne) muszą być zapewnione zgodnie z tymi zasadami. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 2) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 3) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 4) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 5) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 6) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 7) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 8) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 9) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 10) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 11) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).	

	12) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 13) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 14) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 15) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: I. Dystrybucję certyfikatów poprzez http II. Konsolidację CA dla wielu lasów domeny, III. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, IV. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.	

	III. Obsługi 4-KB sektorów dysków IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra V. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. VI. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 16) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 17) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. *Za system równoważny uznaje się system operacyjny, który zapewnia wszystkie wymagane funkcjonalności w sposób natywny lub przy użyciu wbudowanych mechanizmów producenta, bez konieczności zakupu dodatkowych licencji innych producentów.*	
Diagnostyka i Bezpieczeństwo	• zintegrowany z płytą główną moduł TPM 2.0 • Możliwość wyłączenia w BIOS funkcji przycisku zasilania.	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera	
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą: ○ ISO-9001:2015 **(certyfikat załączyć do oferty)** ○ ISO-14001 **(certyfikat załączyć do oferty)** • Serwer musi posiadać deklaracja CE **(załączyć do oferty)** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Server 2022 lub Microsoft Windows Server 2025. **(na potwierdzenie do oferty należy załączyć wydruk ze strony).**	

Warunki gwarancji	24 miesiące gwarancji, realizowanej w miejscu instalacji urządzenia (on-site), z czasem reakcji serwisowej nie dłuższym niż następny dzień roboczy od momentu przyjęcia zgłoszenia. Zgłaszanie awarii musi być możliwe w trybie 24x7x365, za pośrednictwem ogólnodostępnego kanału zgłoszeniowego (telefonicznego lub elektronicznego). W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Serwis gwarancyjny może być realizowany przez producenta urządzenia, autoryzowanego partnera serwisowego producenta lub inny podmiot posiadający równoważny system serwisowy, zapewniający spełnienie wymaganych warunków gwarancji oraz poziomu SLA określonego w niniejszym opisie. Podmiot realizujący serwis powinien posiadać certyfikat ISO 9001:2015 lub równoważny. (**Dokumenty potwierdzające spełnienie wymagań należy dołączyć do oferty.**) W przypadku zaoferowania certyfikatu równoważnego lub innych środków potwierdzających stosowanie równoważnego systemu zarządzania jakością, Wykonawca zobowiązany jest wykazać równoważność poprzez przedstawienie dokumentów potwierdzających, że stosowany system zapewnia poziom zarządzania jakością nie gorszy niż wymagany w normie ISO 9001:2015, w szczególności w zakresie świadczenia usług serwisowych. Wykonawca zobowiązany jest zapewnić możliwość sprawdzenia statusu gwarancji urządzenia przy użyciu unikatowego numeru identyfikacyjnego oraz dostęp do uaktualnień mikrokodu i sterowników producenta, co najmniej w okresie obowiązywania gwarancji.	
Wdrożenie	• Instalacja serwera w miejscu wskazanym przez Zamawiającego • Podłączenie serwerów do zasilania, sieci LAN • Konfiguracja kart zarządzających (IP, powiadomienia email) • Konfiguracja systemu operacyjnego na serwerach • Przygotowanie dokumentacji powdrożeniowej	

III. Wdrożenie usługi serwera logów systemowych i stacji końcowych oraz sieciowych – 7 szt.

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
Wymagania Ogólne	W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: • Amazon Web Service AMI, Amazon EC2, Amazon EBS	

	• Alibaba Cloud
	• Google Cloud Platform
	• IBM Cloud
	• Microsoft Azure
	• Oracle Cloud Infrastructure
	• Citrix XenServer 8.2 and later
	• OpenSource XenServer 4.2.5
	• Microsoft Hyper-V Server 2016, 2019, and 2022
	• Nutanix
	  • AHV 20220304 and later
	  • AOS 6.5 and later
	  • NCC 4.6 and later
	  • LCM 3.0 and later
	• RedHat 9.1
	  • Other versions and Linux KVM distributions are also supported
	• VMware ESXi versions 6.5 and later	

Interfejsy, Dysk	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.	
Parametry wydajnościowe	1. System musi być w stanie przyjmować minimum 2 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.	
Logowanie	1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów , do których nawiązywane są połączenia. f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi	

	być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.	
Raportowanie	W zakresie raportowania system musi zapewniać: 1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.	
Korelacja logów	W zakresie korelacji zdarzeń system musi zapewniać: 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.	
Zarządzanie	1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. 2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.	
Serwisy i licencje	1. System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. 2. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.	

Inne	Zaleca się, aby w przypadku istnienia wymogów prawnych odnoszących się do technologii objętej przedmiotem niniejszego postępowania, w szczególności w zakresie tzw. produktów podwójnego zastosowania, Wykonawca posiadał lub był w stanie przedstawić na żądanie Zamawiającego dokument pochodzący od importera danej technologii, potwierdzający, że przy jej wprowadzeniu na terytorium Rzeczypospolitej Polskiej zostały dochowane wymogi właściwych przepisów prawa, w tym przepisów dotyczących obrotu z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa oraz dla utrzymania międzynarodowego pokoju i bezpieczeństwa, a także dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę wewnętrzny system kontroli, wymagany w ramach wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Zaleca się, aby Wykonawca posiadał lub był w stanie przedstawić na żądanie Zamawiającego dokument w postaci oświadczenia producenta lub autoryzowanego dystrybutora producenta na terytorium Rzeczypospolitej Polskiej, potwierdzający, że oferowany produkt pochodzi z autoryzowanego kanału sprzedaży, w szczególności poprzez wykazanie posiadanego statusu autoryzacyjnego lub innego równoważnego potwierdzenia.	
Wdrożenie	1. Instalacja systemu oraz podpięcie otrzymanej licencji na serwerze dostarczonym w ramach przedmiotowego postepowania (*Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych*) 2. Zdefiniowanie domeny administracyjnej i partycjonowania dysku 3. Konfiguracja warstwy sieciowej (L3, routing, LACP) 4. Konfiguracja ustawień systemowych (konta administratorów, certyfikaty, SMTP) 5. Podłączenie urządzeń zabezpieczenia sieci 6. Przygotowanie instrukcji podłączenia urządzeń sieci komputerowej 7. Ustawienie harmonogramu raportów	

IV. Urządzenie typu NAS na potrzeby kopii wraz z instalacją i konfiguracją – 7 szt.

Nazwa	**Wymagane parametry techniczne**	**Spełnia TAK/NIE**
Procesor	Intel® Celeron® N5095 (or N5105) 4-core/4-thread processor, burst up to 2.9 GHz lub równoważny	
Obudowa	Desktop o wymiarach nie większych niż 166(Wysokość) x 171(Szerokość) x 227 (Głębokość) mm	
Pamięć RAM	16GB RAM DDR4 SODIMM	
Ilość obsługiwanych dysków	4 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s 2 x M.2 2280 PCIe Gen 3 x1	
Dyski	3 dyski o pojemności 12TB każdy zgodne z listą kompatybilności oferowanej macierzy oraz charakteryzujące się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - pamięć cache: minimum 256 MB, - gwarancja: minimum 24 miesięcy,	

	- MTBF: minimum 1 milion godzin, - prędkość transferu wewnętrznego: min. 210MB/s, - usługa odzyskiwania danych	
Interfejsy sieciowe	2 x 2,5 Gigabit sieci Ethernet (2,5G/1G/100M), 2 x 10 Gigabit sieci Ethernet (możliwość uzyskania poprzez dołożenie karty rozszerzeń tego samego producenta)	
Porty	2x USB 2.0, 2 x USB 3.2 Gen 2 typu A, 1x HDMI 2.1	
Złącza PCIe	1x Gniazdo 1: PCIe Gen 3 x2	
Wskaźniki LED	Zasilanie/stan, LAN, USB, HDD1–4	
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1, 5, 5+Spare, 6, 10, Obsługa BITMAP w celu przyspieszenia odbudowy.	
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.	
Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.	
Kompatybilny system operacyjny	Apple Mac OS 10.10 or later Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux IBM AIX 7, Solaris 10 or later UNIX Microsoft Windows 7, 8, 10 and 11 Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022 and 2025	
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP	
Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog	
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów	
Język GUI	Polski	
Gwarancja i serwis	Gwarancja producenta – minimum 24 miesięcy	
Waga	Maksymalnie 3,6 kg (brutto)	
Pobór mocy	Praca poniżej 40.536W / Tryb uśpienia poniżej 21.618W	
System plików	Dyski wewnętrzne ZFS/EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+, exFAT (licencja opcjonalna dla modeli z procesorem ARM)	
iSCSI	Obsługa MPIO & MC/S, SPC-3 persistent reservation	
Liczba kont użytkowników	Do min. 15000	
Liczba grup	Do min. 512	
Maks. liczba połączeń współbieżnych (CIFS)	Maksymalnie 1500	
Liczba udziałów	Do min. 256	
Zasilanie	Zewnętrzny Zasilacz 90 W, 100–240 V	
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.	

V. Backupowy serwer redundancji usług – 1 szt.

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
Obudowa	Obudowa Rack o wysokości max. 1U z możliwością instalacji min. 8 dysków 2,5" NVMe wraz z kompletem szyn wysuwanych umożliwiających montaż w szafie rack. Serwer wyposażony w standardowy zdejmowalny panel przedni z zamkiem chroniącym przed nieuprawnionym dostępem do dysków. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.	
Płyta główna	Płyta główna z możliwością zainstalowania dwóch procesorów. Obsługa procesorów 144 rdzeniowych. Płyta główna powinna obsługiwać do 8TB pamięci RAM w konfiguracji dwuprocesorowej. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.	
Procesor	Zainstalowany procesor min. 16-rdzeniowy klasy x86, 2,3GHz częstotliwości bazowej, dedykowany do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min. 371 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.(lub równoważnym, opublikowanym przez niezależną organizację branżową, dla konfiguracji dwurocesorowej). **(na potwierdzenie do oferty należy załączyć wydruk ze strony dla oferowanego procesora).**	
RAM	Minimum 256 GB pamięci RAM typu DDR5 ECC RDIMM o częstotliwości taktowania minimum 6400 MT/s, z możliwością dalszej rozbudowy. Płyta główna serwera musi umożliwiać instalację pamięci RAM w liczbie slotów pozwalającej na osiągnięcie co najmniej 256 GB pamięci przy zachowaniu parametrów określonych powyżej.	
Gniazda PCIe	Minimum dwa sloty PCIe x16 (Gen5) i dwa sloty OCP 3.0	
Interfejsy sieciowe/FC/SAS	Zainstalowane min. 4 interfejsy sieciowe 1Gb Ethernet w standardzie Base-T oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). Dopuszczalne są porty w slocie OCP. Porty obsadzone modułami 25Gbs SFP+ MM Dostarczenie 2 światłowodów MM OM4 LC-LC o długości minimum 3m.	
Dyski twarde	Zainstalowane 2 x 3.84 TB Data Center NVMe Read Intensive U2 Zainstalowane dwa dyski M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1	
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.	
Wbudowane porty	min. 1 port USB-C oraz 3 x USB 3.1 1 port VGA, Możliwość wyposażenia w dodatkowy port Mini-Displayport	

Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200	
Wentylatory	Redundantne	
Zasilacze	Min. dwa zasilacze Hot-Plug min. 1100W Titanium Kable zasilające: 2x C13/C14 10A 2x Kabel z wtyczką europejską	
Bezpieczeństwo	Serwer wyposażony w zatrzask górnej pokrywy. Blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. Możliwość integracji z RSA SecurID. Jeżeli funkcja wymaga dodatkowej licencji to nie jest ona wymagana na tym etapie postępowania. Moduł TMP 2.0 Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.	
Karta Zarządzania	Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowany port RJ-45 Gigabit Ethernet umożliwiającej: zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer. • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji serwera do pliku XML lub JSON	

	• Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera. Karta powinna umożliwiać rozszerzenie funkcjonalności o: możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • Automatyczne odświeżanie certyfikatów SSL • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe • monitorowanie przepływu powietrza na bieżąco	
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą: o ISO-9001:2015 **(certyfikat załączyć do oferty)** o ISO-14001 **(certyfikat załączyć do oferty)** • Serwer musi posiadać deklaracja CE **(załączyć do oferty)** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Server 2022 lub Microsoft Windows Server 2025. **(na potwierdzenie do oferty należy załączyć wydruk ze strony).**	
Warunki gwarancji	24 miesiące gwarancji, realizowanej w miejscu instalacji urządzenia (on-site), z czasem reakcji serwisowej nie dłuższym niż następny dzień roboczy od momentu przyjęcia zgłoszenia. Zgłaszanie awarii musi być możliwe w trybie 24x7x365, za pośrednictwem ogólnodostępnego kanału zgłoszeniowego (telefonicznego lub elektronicznego). W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Serwis gwarancyjny może być realizowany przez producenta urządzenia, autoryzowanego partnera serwisowego producenta lub inny podmiot posiadający równoważny system serwisowy, zapewniający spełnienie wymaganych warunków gwarancji oraz poziomu SLA określonego w niniejszym opisie. Podmiot realizujący serwis powinien posiadać certyfikat ISO 9001:2015 lub równoważny. (**Dokumenty potwierdzające spełnienie wymagań należy dołączyć do oferty.**) W przypadku zaoferowania certyfikatu równoważnego lub innych środków potwierdzających stosowanie równoważnego systemu zarządzania	

	jakością, Wykonawca zobowiązany jest wykazać równoważność poprzez przedstawienie dokumentów potwierdzających, że stosowany system zapewnia poziom zarządzania jakością nie gorszy niż wymagany w normie ISO 9001:2015, w szczególności w zakresie świadczenia usług serwisowych. Wykonawca zobowiązany jest zapewnić możliwość sprawdzenia statusu gwarancji urządzenia przy użyciu unikatowego numeru identyfikacyjnego oraz dostęp do uaktualnień mikrokodu i sterowników producenta, co najmniej w okresie obowiązywania gwarancji.	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	
Wdrożenie	• Instalacja serwera w miejscu wskazanym przez Zamawiającego • Podłączenie serwerów do zasilania, sieci LAN • Konfiguracja kart zarządzających (IP, powiadomienia email) • Konfiguracja systemu operacyjnego na serwerach • Przygotowanie dokumentacji powdrożeniowej	

VI. Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci – 7 szt.

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
Kluczowe funkcjonalności	1. Rozwiązanie jest systemem heterogenicznym i posiada możliwość instalacji na systemie operacyjnym Windows x64, jak również Linux, 2. Rozwiązanie jest instalowane z własną darmową bazą danych postgreSQL, z możliwością migracji do komercyjnej bazy danych MS SQL, 3. Rozwiązanie wspiera integrację Active Directory, LDAP 4. Rozwiązanie pozwala na import grup z AD 5. Rozwiązanie posiada własny wbudowany interfejs, przez który odbywa się konfiguracja bazy danych 6. Rozwiązanie integruje się z dowolną skrzynką pocztową działająca na protokole POP, POPS, IMAP, IMAPS, SMTP, SMTPS, jak również obsługuje Exchange Web Services (EWS), 7. Rozwiązanie wspiera możliwość logowania bez potrzeby ponownego używania poświadczeń do aplikacji dzięki autentykacji poprzez SAML 2.0 Single Sign On (SAML SSO), 8. Aplikacja posiada możliwość uruchomienia dwuskładnikowego logowania przy użyciu Emaila lub gogle Authenticator'a 9. Aplikacja pozwala na podpięcie certyfikatów SSL 10. Aplikacja działa na bazie dostępnych ról uprawniających do pracy w narzędziu	

Możliwości oprogramowania	1. Rozwiązanie posiada własny wbudowany moduł raportowania wzbogacony o możliwość kewrendowania do bazy danych, 2. Rozwiązanie wspiera przeglądarki – IE Edge, Chrome, Firefox 3. Dostęp do systemu dla użytkownika jest zapewniony za pośrednictwem konsoli webowej lub z aplikacji mobilnej	
Funkcjonalności	1. Rozwiązanie posiada Centralną bazę zasobów, oprogramowania oraz bazę CMDB wraz ze zintegrowanym wykrywaniem środowiska IT 2. Rozwiązanie umożliwia przechowywanie danych o wszystkich jednostkach konfiguracji (CI) takich jak: • Komputery • Drukarki sieciowe • Urządzenia sieciowe (przełączniki, routery, firewalle, access pointy, adresy IP, MAC) • Pakiety oprogramowania • Komponenty komputerów i urządzeń sieciowych • Usługi biznesowe oraz IT • Zasoby ludzkie (np. użytkownicy, grupy użytkowników, serwisanci, grupy serwisowe) 3. Rozwiązanie zawiera gotowy schemat danych wraz z listą możliwych relacji pomiędzy jednostkami konfiguracji, jak również możliwość rozbudowanie go o własne, zdefiniowane relacje 4. Rozwiązanie umożliwia dynamiczne rozszerzenie schematu danych o dodatkowe atrybuty, w tym atrybuty dedykowane dla konkretnego typu jednostki konfiguracji CI. Rozszerzenie odbywa się z poziomu interfejsu graficznego systemu. 5. Rozwiązanie umożliwia przedstawienie w sposób graficzny wzajemnych relacji pomiędzy jednostki konfiguracji CI. 6. Rozwiązanie umożliwia przechowywanie informacji pomiędzy incydentami, problemami oraz zmianami, a jednostkami konfiguracji 7. Rozwiązanie umożliwia ręczne dodawanie jednostek konfiguracji oraz relacji pomiędzy nimi z poziomu interfejsu graficznego jak również importu danych o jednostkach konfiguracji z plików w formacie CSV lub XML 8. Rozwiązanie posiada zintegrowany moduł wykrywania środowiska IT, pozwalający na wykrycie co najmniej konfiguracji komputerów, serwerów i oprogramowania. Wykrywanie opiera się na wykorzystaniu skanowania agentowego. 9. Rozwiązanie umożliwia przechowywanie informacji o poszczególnych elementach konfiguracji w taki sposób, by możliwe było rejestrowanie i śledzenie historii posiadania elementu konfiguracji przez użytkowników, powiązanie z nim informacji o koszcie zakupu, innych kosztach eksploatacyjnych, warunkach umowy serwisowej, dostawcą 10. Rozwiązanie umożliwia wyszukiwanie elementów konfiguracji po dowolnych atrybutach, zarówno standardowych, jaki i dodanych przez użytkownika, w tym po kodach kreskowych 11. Rozwiązanie umożliwia zdefiniowanie wartości początkowej elementu konfiguracji oraz mierzenie jego amortyzacji. 12. Rozwiązanie umożliwia powiązanie poszczególnych elementów konfiguracji z danymi użytkownika (jego imieniem i nazwiskiem, nr	

telefonu, departamentem), departamentu, innymi elementami konfiguracji i katalogiem usług.

13. Rozwiązanie umożliwia przechowywanie informacji o posiadanych przez użytkownika licencjach na oprogramowanie, powiązać posiadane licencje z zainstalowanym na komputerach oprogramowaniem oraz rejestrować historię zmian posiadania danej licencji
14. Rozwiązanie umożliwia zarządzanie licencjami na oprogramowanie posiadane przez użytkowników w tym zarządzanie umowami dotyczącymi zakupu licencji oraz zasilanie CMDB danymi dotyczącymi licencji pochodzącymi z innych źródeł danych.
15. Rozwiązanie umożliwia wygenerowanie raportu posiadanych licencji przez użytkownika oraz raportów zgodności licencji z zainstalowanym oprogramowaniem
16. Rozwiązanie umożliwia z poziomu interfejsu oprogramowania nawiązanie sesji zdalnej w trybie przejęcia pulpitu użytkownika z komputerem przechowywanym w bazie
17. Rozwiązanie posiada API
18. Rozwiązanie posiada moduł wykrywania środowiska, który umożliwia zbieranie danych o konfiguracji komputerów, co najmniej:
    - Ilości i rodzaju procesora
    - Wielkość dostępnej pamięci fizycznej i wirtualnej
    - Nr seryjnego komputera
    - Nazwa i wersja systemu operacyjnego
    - Zainstalowane oprogramowanie i poprawki
19. Rozwiązanie posiada mechanizm generowania kodów kreskowych dla zasobów. Moduł pozwala na zdefiniowanie formatu kodu kreskowego i jego wydruk według zdefiniowanego formatu wydruku.
20. Rozwiązanie posiada możliwość wprowadzania zasobów skanowanych po kodzie kreskowym
21. Rozwiązanie umożliwia przeprowadzenie wykrywania zmian w konfiguracji i generowania raportów porównawczych zmian w elementach konfiguracji
22. Rozwiązanie umożliwia przeprowadzenie automatycznych, zdefiniowanych według cyklicznego harmonogramu audytów konfiguracji komputerów i serwerów, pod kątem zmian w konfiguracji i zainstalowanym oprogramowaniu
23. Rozwiązanie umożliwia przeprowadzenie skanowania komputerów i zasilenie danych do bazy dla komputerów niepodłączonych do sieci komputerowej. Możliwe jest zastosowanie specjalnych skryptów, których plik wynikowy następnie zostanie zaimportowany do bazy.
24. System posiada możliwość zarządzania umowami serwisowymi dla elementów konfiguracji (CI) przechowywanych w bazie konfiguracji CMDB
25. Rozwiązanie w ramach zarządzania umowami posiada możliwość tworzenia umów, przegląd, edycje oraz usuwanie
26. Moduł zarządzania umowami serwisowymi umożliwia rejestrację warunków umów gwarancyjnych i serwisowych, w tym w szczególności dane teleadresowe gwaranta, czas obowiązywania umowy, jej koszt, warunki na jakich umowa jest świadczona oraz

	powiązania ich z jednym lub wieloma elementami konfiguracji bazy CMDB 27. Moduł zarządzania umowami serwisowymi posiada funkcjonalność pozwalającą przesyłać powiadomienia o wygaśnięciu okresu obowiązywania umowy serwisowej i gwarancyjnej 28. Rozwiązanie w ramach zarządzania umowami posiada możliwość dołączenia załączników 29. Rozwiązanie w ramach zarządzania umowami posiada możliwość tworzenia tzw. Umów podrzędnych do głównej umowy. 30. Rozwiązanie w ramach zarządzania umowami pozwala na tworzenie dodatkowych pól niezbędnych i wymaganych przez organizacji 31. Moduł zarządzania zakupami umożliwia przeprowadzenie procesu zakupowego składającego się z co najmniej następujących kroków: • Utworzenie zamówienie – rejestracja numeru zamówienia, powiązanie z dostawcą, określenie terminu realizacji zamówienia • Dodanie pozycji do zamówienia – rejestracja produktów, ich ilości oraz ceny jednostkowej produktu • Przedstawienie zamówienia do akceptacji – moduł zarządzania zakupami umożliwia przeprowadzenie weryfikacji i akceptacji zamówienia przez osoby trzecie, z tymże użytkownik rejestrujący zamówienie nie może być jednocześnie osobą trzecią weryfikującą i akceptującą realizację zamówienia • Powiązanie zamówienia z elementami konfiguracji w bazie CMDB • Moduł zarządzania zakupami umożliwia przesłanie powiadomienia do osób trzecich o przekroczonym terminie realizacji zamówienia 32. Aplikacja pozwala zarządzać procesem wypożyczenia sprzętu 33. Aplikacja pozwala na budowanie i nadzorowanie magazynu sprzętu 34. Aplikacja pozwala na generowanie grup w oparciu o kryteria 35. Możliwość spięcia poczty za pomocą Microsoft Graph	
Licencja	Licencja wieczysta, powinna umożliwiać zinwentaryzowanie w systemie ilości zasobów zarządzanych – IT Assets (zasobów posiadających adres IP) w ilości określonej w *Części B. Przedmiot zamówienia* dla każdej instalacji. Wparcie producenta w okresie 12 miesięcy.	
Wdrożenie	1. Instalacja aplikacji oraz podpięcie otrzymanej licencji na serwerze dostarczonym w ramach przedmiotowego postepowania (*Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych*) 2. Rekonfiguracja aplikacji w zakresie korzystania z protokołu https 3. Dodanie 2 techników z przygotowaniem dla nich ról 4. Przygotowanie agenta i dystrybucja na dwóch komputerach przy pomocy GPO(AD) lub 5. instalacja na 2 komputerach manualnie, 6. Konfiguracja skanowania sieci dla jednej z wybranych metod (WMI, Telnet/SSH, SNMP, lub VMWare)	

	7. Przygotowanie pliku csv i import do 10 zasobów 8. Konfiguracja jednej umowy licencyjnej i podpięcie jej pod zasób 9. Konfiguracja jednej umowy i omówienie procesu zakupu 10. Przygotowanie dwóch typów elementu konfiguracyjnego wraz z wzajemnymi powiązaniami 11. Wstęp do obsługi aplikacji a także omówienie metod zapewnienia ciągłości działania (backup, restore, update)	

VII. Wdrożenie rozwiązań XDR i SIEM do monitoringu stacji końcowych – 8 szt.

VII.A. System XDR

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
Administracja zdalna	1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS). 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej: 5.1. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania, 5.2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta, 5.3. Buforowanie ruchu HTTPS. 6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej. 7.1. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android: 7.1.1. Google Authenticator, 7.1.2. Microsoft Authenticator, 7.1.3. Authy, 7.1.4. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania. 8. Rozwiązanie musi posiadać minimum 80 szablonów raportów,	

	przygotowanych przez producenta. 9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 9.1. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: 9.1.1. adresy sieciowe IP, 9.1.2. aktywne zagrożenia, 9.1.3. stan funkcjonowania oraz ochrony, 9.1.4. wersja systemu operacyjnego, 9.1.5. podzespoły komputera. 10. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem: 10.1. wyrażenie CRON, 10.2. codziennie, 10.3. cotygodniowo, 10.4. co miesiąc, 10.5. co rok, 10.6. po wystąpieniu nowego zdarzenia, 10.7. po automatycznym umieszczeniu hosta w grupie dynamicznej. 11. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim 11.1. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania 12. Rozwiązanie musi mieć możliwość tagowania obiektów. 13. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog. 13.1. Eksport danych musi być możliwy w co najmniej następujących formatach: 13.1.1. JSON, 13.1.2. LEEF, 13.1.3. CEF.	
Ochrona stacji roboczych - Windows	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: 3.1. wirus, 3.2. trojan,	

3.3. robak,
3.4. adware,
3.5. spyware,
3.6. dialer,
3.7. phishing,
3.8. backdoor.

4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
   7.1. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
   7.2. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
   7.3. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    10.1. całego dysku,
    10.2. wybranych katalogów,
    10.3. pojedynczych plików,
    10.4. plików spakowanych oraz skompresowanych,
    10.5. dysków sieciowych,
    10.6. dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    11.1. wybranych plików,
    11.2. wybranych procesów,
    11.3. wybranych lokalizacji,
    11.4. wybranych rozszerzeń,
    11.5. nazwy wykrycia,
    11.6. sumy kontrolnej (SHA1).
12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania

antywirusowego, który umożliwia co najmniej:

13.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.

13.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

13.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

14. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

17.1. typ urządzenia:

17.1.1. pamięci masowe,
17.1.2. optyczne pamięci masowe,
17.1.3. pamięci masowe Firewire,
17.1.4. urządzenia do tworzenia obrazów,
17.1.5. drukarki USB,
17.1.6. urządzenia Bluetooth,
17.1.7. czytniki kart inteligentnych,
17.1.8. modemy,
17.1.9. porty LPT/COM,
17.1.10. urządzenia przenośne.

17.2. parametry urządzenia:

17.2.1. numer seryjny,
17.2.2. producent,
17.2.3. model.

17.3. typ dostępu:

17.3.1. brak możliwości zapisu,
17.3.2. pełen dostęp,
17.3.3. ostrzeżenie użytkownika,
17.3.4. brak dostępu.

18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

18.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i

wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

18.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

18.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

18.4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

18.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

19.1. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

19.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

19.3. Raport musi posiadać co najmniej:

19.3.1. Listę zainstalowanych aplikacji,

19.3.2. Listę usług systemowych,

19.3.3. Informacje o systemie operacyjnym i sprzęcie,

19.3.4. Listę aktywnych procesów i połączeń sieciowych,

19.3.5. Harmonogram systemu operacyjnego,

19.3.6. Szczegóły pliku hosts,

19.3.7. Informacje o sterownikach.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu

20.1. antywirus,

20.2. zapora osobista

20.3. sandbox,

20.4. antyspyware,
20.5. metody heurystyczne.
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
22.1. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
22.2. Ochrona musi być realizowana w oparciu o co najmniej:
22.2.1. globalna czarna lista RBL,
22.2.2. czarna lista użytkownika,
22.2.3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
23.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
23.1.1. Skanowanie portów TCP oraz UDP,
23.1.2. Wykrywanie duplikacji adresu IP,
23.1.3. Atak zatruwania ARP,
23.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.
23.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
23.2.1. RDP,
23.2.2. SMB,
23.2.3. My SQL,
23.2.4. MS SQL.
23.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
24.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
24.2. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
24.2.1. tryb automatyczny - rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
24.2.2. tryb interaktywny - rozwiązanie pyta się o każde nowo nawiązywane połączenie,
24.2.3. tryb oparty na regułach - rozwiązanie blokuje

	ruch przychodzący i wychodzący, 24.2.4. tryb uczenia się - rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. 24.2.4.1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu. 25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego. 25.1. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 25.2. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 25.3. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu. 26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta. 26.1. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii. 26.2. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: 26.2.1. Treść komunikatu, 26.2.2. Obraz.	
Ochrona stacji roboczych - MacOS	1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych. 2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: 3.1. wirus, 3.2. trojan, 3.3. robak, 3.4. adware, 3.5. spyware, 3.6. dialer, 3.7. phishing, 3.8. backdoor. 4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły	

heurystyczne - jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie.

5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi chronić pliki co najmniej za pomocą:
   6.1. Sygnatur wirusów.
   6.2. Reputacji chmurowej.
7. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   8.1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
   8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   9.1. całego dysku,
   9.2. wybranych katalogów,
   9.3. pojedynczych plików,
   9.4. plików spakowanych oraz skompresowanych,
   9.5. Dysków sieciowych,
   9.6. dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    10.1. wybranych plików,
    10.2. wybranych procesów,
    10.3. wybranych lokalizacji,
    10.4. wybranych rozszerzeń,
    10.5. nazwy wykrycia,
    10.6. sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
    11.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.
    11.2. Zapora osobista musi posiadać co najmniej dwa tryby pracy:

	11.2.1. tryb automatyczny - rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące, 11.2.2. tryb oparty na regułach - rozwiązanie blokuje ruch przychodzący i wychodzący,	
Ochrona stacji roboczych - Linux	1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne: 1.1. Ubuntu Desktop, 1.2. Red Hat Enterprise Linux 1.3. Linux Mint. 2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu: 2.1. Cinnamon, 2.2. GNOME, 2.3. KDE, 2.4. MATE, 2.5. XFCE. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: 3.1. wirus, 3.2. trojan, 3.3. robak, 3.4. adware, 3.5. spyware, 3.6. dialer, 3.7. phishing, 3.8. backdoor. 4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie. 5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej: 6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników. 6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. 7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: 7.1. całego dysku,	

	7.2. wybranych katalogów, 7.3. pojedynczych plików, 7.4. plików spakowanych oraz skompresowanych, 7.5. dysków sieciowych, 7.6. dysków przenośnych. 8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: 8.1. wybranych plików, 8.2. wybranych procesów, 8.3. wybranych lokalizacji, 8.4. wybranych rozszerzeń, 9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej: 9.1. typ urządzenia: 9.1.1. pamięci masowe, 9.1.2. optyczne pamięci masowe, 9.2. parametry urządzenia: 9.2.1. numer seryjny, 9.2.2. producent, 9.2.3. model. 9.3. typ dostępu: 9.3.1. brak możliwości zapisu, 9.3.2. pełen dostęp, brak dostępu.	
Ochrona serwera - Windows Server	1. Rozwiązanie musi wspierać systemy w tym co najmniej: 1.1. Microsoft Windows Server 2012 R2, 1.2. Microsoft Windows Server 2016, 1.3. Microsoft Windows Server 2019, 1.4. Microsoft Windows Server 2022, 1.5. Microsoft Windows Server 2025. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: 3.1. wirus, 3.2. trojan, 3.3. robak, 3.4. adware, 3.5. spyware, 3.6. dialer, 3.7. phishing, 3.8. backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły	

heurystyczne - jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   8.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
   8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   9.1. całego dysku,
   9.2. wybranych katalogów,
   9.3. pojedynczych plików,
   9.4. plików spakowanych oraz skompresowanych,
   9.5. dysków sieciowych,
   9.6. dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   10.1. wybranych plików,
   10.2. wybranych procesów,
   10.3. wybranych lokalizacji,
   10.4. wybranych rozszerzeń,
   10.5. nazwy wykrycia,
   10.6. sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
   12.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
   12.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
   12.3. tryb oparty na regułach, gdzie zastosowanie mają

jedynie reguły utworzone przez użytkownika,

12.4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

12.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
    13.1. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
    13.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
    13.3. Raport musi posiadać co najmniej:
        13.3.1. Listę zainstalowanych aplikacji,
        13.3.2. Listę usług systemowych,
        13.3.3. informacje o systemie operacyjnym i sprzęcie,
        13.3.4. Listę aktywnych procesów i połączeń sieciowych,
        13.3.5. harmonogram systemu operacyjnego,
        13.3.6. Szczegóły pliku hosts,
        13.3.7. Informacje o sterowników.
14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
    14.1. antywirus,
    14.2. zapora osobista
    14.3. sandbox,
    14.4. antyspyware,
    14.5. metody heurystyczne.
15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz

grup urządzeń na stacji w oparciu o co najmniej:

17.1. typ urządzenia:
- 17.1.1. pamięci masowe,
- 17.1.2. optyczne pamięci masowe,
- 17.1.3. pamięci masowe Firewire,
- 17.1.4. urządzenia do tworzenia obrazów,
- 17.1.5. drukarki USB,
- 17.1.6. urządzenia Bluetooth,
- 17.1.7. czytniki kart inteligentnych,
- 17.1.8. modemy,
- 17.1.9. porty LPT/COM,
- 17.1.10. urządzenia przenośne.

17.2. parametry urządzenia:
- 17.2.1. numer seryjny,
- 17.2.2. producent,
- 17.2.3. model.

17.3. typ dostępu:
- 17.3.1. brak możliwości zapisu,
- 17.3.2. pełen dostęp,
- 17.3.3. ostrzeżenie użytkownika,
- 17.3.4. brak dostępu.

18. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
- 18.1. MS SQL,
- 18.2. Active Directory,
- 18.3. IIS,
- 18.4. Sysvol,
- 18.5. DNS,
- 18.6. DHCP,
- 18.7. Hyper-V,
- 18.8. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.

19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

19.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
- 19.1.1. Skanowanie portów TCP oraz UDP,
- 19.1.2. Wykrywanie duplikacji adresu IP,
- 19.1.3. Atak zatruwania ARP,
- 19.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.

19.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
- 19.2.1. RDP,
- 19.2.2. SMB,

	19.2.3. My SQL, 19.2.4. MS SQL. 19.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego. 21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta. 21.1. Zapora osobista musi posiadać co najmniej cztery tryby pracy: 21.1.1. tryb automatyczny - rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące, 21.1.2. tryb interaktywny - rozwiązanie pyta się o każde nowo nawiązywane połączenie, 21.1.3. tryb oparty na regułach - rozwiązanie blokuje ruch przychodzący i wychodzący, 21.1.4. tryb uczenia się - rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. 21.1.4.1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.	
Ochrona serwera - Linux	1. Rozwiązanie musi wspierać systemy w tym co najmniej: 1.1. RedHat Enterprise Linux (RHEL), 1.2. Rocky Linux, 1.3. Ubuntu, 1.4. Debian, 1.5. SUSE Linux Enterprise Server (SLES), 1.6. Oracle Linux, 1.7. Amazon Linux. 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: 2.1. wirus, 2.2. trojan, 2.3. robak, 2.4. adware, 2.5. spyware, 2.6. dialer, 2.7. phishing, 2.8. backdoor. 3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS. 4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły	

heurystyczne - jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie.

5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   7.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   7.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   8.1. całego dysku,
   8.2. wybranych katalogów,
   8.3. pojedynczych plików,
   8.4. plików spakowanych oraz skompresowanych,
   8.5. dysków sieciowych,
   8.6. dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   9.1. wybranych plików,
   9.2. wybranych procesów,
   9.3. wybranych lokalizacji,
   9.4. wybranych rozszerzeń,
10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
    10.1. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
12. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
    13.1. proces budowania obrazu kontenera,

	13.2. wdrażanie obrazu kontenera.	
Mobile Device Management	1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi - MDM. 2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania. 2.1. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami: 2.1.1. Android 2.1.2. iOS, 2.1.3. iPadOS. 2.2. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami: 2.2.1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników), 2.2.2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania), 2.2.3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania), 2.2.4. Apple Business Manager (ABM), 2.2.5. Android Enterprise (co najmniej w zakresie Device Owner). 3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: 3.1. usunięcie zawartości urządzenia, 3.2. przywrócenie urządzenia do ustawień fabrycznych, 3.3. zablokowanie urządzenia, 3.4. uruchomienie sygnału dźwiękowego, 3.5. lokalizację GPS, 3.6. Resetowanie hasła blokady ekranu. 4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 5. MDM musi umożliwiać co najmniej: 5.1. Dla systemów iOS oraz iPadOS 5.1.1. konfigurację kont e-mail, 5.1.2. konfigurację połączeń VPN, 5.1.3. Konfigurację połączeń Wi-Fi, 5.1.4. Konfigurację listy certyfikatów, 5.1.5. możliwość uruchomienia trybu jednej aplikacji. 5.2. Dla systemu Android:	

	5.2.1. blokadę wykonywania połączeń, 5.2.2. blokadę konfiguracji sieci Wi-Fi, 5.2.3. blokadę konfiguracji tuneli VPN, 5.2.4. zarządzenie aktualizacjami sytemu operacyjnego, 5.2.5. blokadę zmiany tapety urządzenia. **Mobile Threat Defense (MTD) dla systemu Android** 1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: 2.1. Inteligentne - tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD. 2.2. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej: 4.1. Złożoność kodu blokady ekranu: 4.1.1. Wzór, 4.1.2. PIN, 4.1.3. Hasło 4.2. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu, 4.3. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu. 5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: 5.1. nazwę aplikacji, 5.2. nazwę pakietu, 5.3. kategorię sklepu Google Play, 5.4. uprawnienia aplikacji, 5.5. pochodzenie aplikacji z nieznanego źródła. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.	
Sandbox	1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń. 2. Dopuszcza się aby Sandbox realizowany był przez usługę chmurową producenta. 3. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego. 4. Rozwiązanie musi wspierać systemy w tym co najmniej: 4.1. Microsoft Windows 10 oraz 11,	

4.2. Microsoft Windows Server,
4.3. macOS 11 (Big Sur) oraz nowszych
4.4. RedHat Enterprise Linux (RHEL),
4.5. Rocky Linux,
4.6. Ubuntu,
4.7. Debian,
4.8. SUSE Linux Enterprise Server (SLES),
4.9. Oracle Linux,
4.10. Amazon Linux.

5. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
6. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
7. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
   7.1. archiwa,
   7.2. skrypty,
   7.3. pliki wykonywalne,
   7.4. pliki rejestru systemowego (.reg),
   7.5. możliwy spam,
   7.6. dokumenty.
8. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
   8.1. natychmiast po ich przeanalizowaniu,
   8.2. po upływie 30 dni,
   8.3. nigdy.
9. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
10. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
11. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
12. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
13. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
    13.1. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
14. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
    13.1. czysty,
    13.2. podejrzany,

	13.3. bardzo podejrzany, 13.4. szkodliwy. 15. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej: 15.1. wstrzymania uruchamiania pobieranych plików z następujących źródeł: 15.1.1. przeglądarki internetowe, 15.1.2. programy poczty e-mail, 15.1.3. nośniki wymienne, 15.1.4. pliki wyodrębnione z archiwum. 16. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.	
eXtended Detection and Response (XDR)	Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego: 3.1. tworzenie procesów, 3.2. uruchamianie, zatrzymanie i modyfikacja usług, 3.3. utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym, 3.4. usuwanie oraz zmiana nazw plików, 3.5. tworzenie i usuwanie kluczy rejestru systemowego, 3.6. ładowanie bibliotek DLL, 3.7. zalogowanie użytkowników, 3.8. elementy sieciowe, w tym co najmniej 3.8.1. pobranie plików wykonywalnych, 3.8.2. zestawienie połączeń TCP/IP, 3.8.3. zapytania HTTP, 3.8.4. zapytania DNS. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. 4.1. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach: 4.1.1. blokowanie pliku wykonywalnego, 4.1.2. blokowanie pliku wykonywalnego i poddanie	

go kwarantannie,

4.1.3. blokowanie podejrzanej biblioteki DLL,

4.1.4. zakończenie procesu,

4.1.5. skanowanie komputera w poszukiwaniu zagrożeń,

4.1.6. wyłączenie komputera,

4.1.7. izolacja sieciowa hosta,

4.1.8. wylogowanie użytkownika.

4.2. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.

Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5.1. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.

5.2. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:

5.2.1. proces,

5.2.2. proces nadrzędny (proces rodzica),

5.2.3. nazwę procesu,

5.2.4. ścieżkę procesu,

5.2.5. wiersz polecenia,

5.2.6. wydawcę,

5.2.7. typ podpisu,

5.2.8. SHA-1,

5.2.9. SHA-2,

5.2.10. użytkownika

5.3. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.

6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.

6.1. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.

6.2. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):

6.2.1. SHA-1,

6.2.2. SHA-256.

7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:

7.1. hash pliku SHA-1,

7.2. hash pliku SHA-256,

7.3. hash pliku MD5,

	7.4. typ sygnatury podpisu cyfrowego, 7.5. wydawcę certyfikatu, 7.6. wersję pliku, 7.7. oryginalną nazwę pliku, 7.8. rozmiar pliku, 7.9. reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego, 7.10. pierwsze uruchomienie pliku w środowisku, 7.11. ostatnie uruchomienie pliku w środowisku, 8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL: 8.1. oznaczania ich jako bezpieczne lub niebezpieczne, 8.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem, 8.3. zablokowania wykonywania i wykorzystania pliku, 8.4. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego. 9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń). 9.1. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 9.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem, 9.3. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego. 9.4. administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera. 10.1. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli. 11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów. 12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.	
Szyfrowanie*	1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.	

	2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker. 3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego. 5. Rozwiązanie musi posiadać autentykacje typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. 5.1. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia. 5.2. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania. 6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania. 6.1. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane. 6.2. Hasło odzyskiwania nie może być krótsze niż 8 znaków. 6.3. Hasło odzyskiwania nie może być dłuższe niż 20 znaków. 7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. 8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory. 9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0. 10. Rozwiązanie musi wspierać dyski wykorzystującego funkcji OPAL w wersji co najmniej 2.0. 11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku. **/*Zaoferowanie funkcjonalności szyfrowania stanowi kryterium dodatkowe/**	
Licencja	Licencja w ilości określonej w *Części B. Przedmiot zamówienia* dla każdej instalacji na okres 12 miesięcy.	
Wdrożenie	1. Instalacja i konfiguracja serwera zarządzającego. Zamawiający dopuszcza realizację systemu zarządzania zarówno w modelu lokalnym (on-premises), jak i w modelu opartym o konsolę zarządzającą udostępnianą w chmurze przez producenta oprogramowania, pod warunkiem zapewnienia pełnej funkcjonalności zarządzania, monitorowania oraz raportowania. 2. Wdrożenie agentów i produktów na urządzeniach: Wykonawca przygotuje pakiety instalacyjne i przeprowadzi przykładową na 20 szt. instalację agentów oraz produktów na wskazanych stacjach i serwerach.	

	3. Konfiguracja polityk bezpieczeństwa: Wykonawca utworzy i przypisze polityki ochrony. 4. Uruchomienie funkcji: Wykonawca wdroży i skonfiguruje reguły detekcji, alerty i powiadomienia o incydentach. 5. Monitorowanie, raportowanie i szkolenie: Wykonawca skonfiguruje alerty i raporty.	

VII.B. System SIEM

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
	Wdrożenie rozwiązania klasy SIEM, przeznaczonego do pracy w środowisku przetwarzającym do 6 GB logów dziennie. Zaoferowane rozwiązanie może stanowić rozbudowę „usługi serwera logów systemowych i stacji końcowych oraz sieciowych" opisanej w poz. III polegającej na jego rozszerzeniu o funkcjonalności **systemu klasy SIEM**, w szczególności w zakresie: • korelacji zdarzeń bezpieczeństwa, • zaawansowanej analizy zagrożeń, • obsługi i automatyzacji reakcji na incydenty (SOAR), • rozszerzonego raportowania bezpieczeństwa. Zamawiający dopuszcza również rozwiązania równoważne, pod warunkiem zapewnienia funkcjonalności nie mniejszej niż określona w opisie przedmiotu zamówienia przy zapewnieniu możliwości integracji z „usługą serwera logów systemowych i stacji końcowych oraz sieciowych" opisaną w poz. III	
Raportowanie bezpieczeństwa	System udostępnia predefiniowane, zaawansowane raporty bezpieczeństwa Możliwość generowania raportów okresowych (cyklicznych) Możliwość generowania raportów na żądanie (ad-hoc) Możliwość eksportu raportów do formatów PDF i CSV	
Obsługa zdarzeń bezpieczeństwa	System umożliwia definiowanie reguł obsługi zdarzeń bezpieczeństwa System automatycznie identyfikuje incydenty na podstawie reguł System generuje alerty i powiadomienia o incydentach	
Korelacja zdarzeń	System realizuje korelację zdarzeń z wielu źródeł logów System posiada predefiniowane reguły korelacji zdarzeń Reguły korelacji umożliwiają wykrywanie złożonych, wieloetapowych zagrożeń Reguły korelacji są aktualizowane w okresie obowiązywania subskrypcji	
Automatyzacja reakcji na incydenty	System udostępnia gotowe scenariusze reakcji (playbooki) składających się z reakcji i sekwencji zautomatyzowanych działań System umożliwia automatyczne wykonanie działań po wykryciu incydentu System umożliwia półautomatyczną reakcję (zatwierdzaną przez operatora) System umożliwia integrację z innymi elementami infrastruktury bezpieczeństwa	
Wdrożenie	1. Konfiguracja nowych raportów zgodnie z dobrymi praktykami i wiedzą wdrożeniową Wykonawcy 2. Konfiguracja przykładowych playbooków 3. Przygotowanie automatyzacji incydentów	
Licencja	Licencja na okres 12 miesięcy.	

VIII. Zestaw dysków do przechowywania kopii zapasowych

Nazwa	Wymagane parametry techniczne	Spełnia TAK/NIE
Opis	**Osiem (8) sztuk** dysków twardych klasy enterprise HDD 3,5" przeznaczonych do zastosowań serwerowych i systemów pamięci masowej w środowisku ciągłej pracy (24/7)	
Pojemność	Minimalna pojemność: 12 TB (terabajtów) przy formatowaniu natywnym	
Format i interfejs	• Format: 3,5 cala; • Interfejs komunikacyjny: SATA III 6 Gb/s (zgodny wstecz z SATA II).	
Prędkość i wydajność	• Prędkość obrotowa talerzy: 7200 RPM; • Bufor pamięci (cache): min. 512 MB; • Maksymalna liniowa prędkość transferu danych: min. 260 MB/s (lub równoważna potwierdzona przez producenta).	
Parametry pracy i niezawodność	• Zastosowanie: praca ciągła 24/7 (Enterprise/Data Center); • Średni czas między awariami (MTBF): min. 2 000 000 godzin; • Obciążalność operacyjna rocznie: min. 550 TB/rok; • Temperatura pracy: zgodna ze specyfikacją producenta do zastosowań serwerowych; • Głośność i wibracje – zgodna ze standardami klasy enterprise HDD.	
Zgodności i standardy	• Zgodność z protokołem SATA III; • Zgodność z systemami monitoringu S.M.A.R.T. oraz narzędziami diagnostycznymi producenta; • Obsługa funkcji zabezpieczeń i optymalizacji pracy dla systemów RAID.	
Gwarancja	• Minimum 24 miesiące gwarancji producenta z opcją naprawy lub wymiany na nowy dysk w przypadku awarii w okresie gwarancyjnym; • Usługi gwarancyjne realizowane przez autoryzowany serwis na terenie Polski.	
Dokumentacja i oznakowanie	• Producent, model, numer katalogowy muszą być jednoznacznie oznaczone na opakowaniu i dysku; • Dołączona instrukcja obsługi oraz karta gwarancyjna w języku polskim lub angielskim; • Certyfikaty zgodności CE, RoHS lub równoważne. • Dysk musi być fabrycznie nowy, pochodzić z legalnej dystrybucji, wolny od wad fizycznych i programowych, dostarczony wraz z pełną dokumentacją producenta oraz gwarancją producenta.	

Część B. Przedmiot zamówienia

Wszystkie wymienione poniżej urządzenia, systemy oraz usługi wdrożeniowe muszą zostać dostarczone, zainstalowane, skonfigurowane oraz uruchomione w lokalizacjach wskazanych w

niniejszym wykazie, tj. w poszczególnych jednostkach organizacyjnych Zamawiającego na terenie miasta Ciechocinek.

Wykonawca zobowiązany jest do realizacji dostaw oraz wdrożeń bezpośrednio w siedzibach wskazanych jednostek, z uwzględnieniem ich istniejącej infrastruktury technicznej i organizacyjnej, a także do zapewnienia prawidłowego działania dostarczonych rozwiązań w każdej z lokalizacji.

Zakres dostawy i wdrożenia dla każdej lokalizacji obejmuje elementy wyszczególnione poniżej, przypisane do danej jednostki organizacyjnej.

Dla każdej z lokalizacji wskazanych w niniejszym wykazie dopuszcza się oraz przewiduje dokonywanie odbiorów częściowych, obejmujących dostawę, instalację, konfigurację oraz uruchomienie urządzeń, systemów i usług wdrożeniowych przypisanych do danej jednostki organizacyjnej.

Odbiór częściowy dla danej lokalizacji następuje po potwierdzeniu przez Zamawiającego prawidłowego i kompletnego wykonania zakresu rzeczowego przewidzianego dla tej lokalizacji oraz zostaje potwierdzony odrębnym protokołem odbioru częściowego.

Odbiory częściowe nie wyłączają prawa Zamawiającego do dokonania odbioru końcowego całości przedmiotu zamówienia po zakończeniu realizacji wszystkich prac objętych umową.

1. **Urząd Miasta w Ciechocinku - ul. Mikołaja Kopernika 19, 87-720 Ciechocinek**
    1) Backupowy serwer redundancji usług (poz. V) – 1 szt.
    2) Wdrożenie rozwiązań XDR (15 stanowisk) i SIEM do monitoringu stacji końcowych (poz. VII) – 1 szt.
    3) Zestaw dysków do przechowywania kopii zapasowych (poz. VIII) – 1 szt.
2. **Ośrodek Sportu i Rekreacji w Ciechocinku, ul. Tężniowa 6, 87-720 Ciechocienk**
    1) Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ II (poz. I.2.) – 1 szt.
    2) Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ II (poz. II.2) – 1 szt.
    3) Wdrożenie usługi serwera logów systemowych i stacji końcowych oraz sieciowych (poz. III) – 1 szt.
    4) Urządzenie typu NAS na potrzeby kopii wraz z instalacją i konfiguracją (poz. IV) – 1 szt.
    5) Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (poz. VI) – system obejmujący 25 zasobów
    1) Wdrożenie rozwiązań XDR (5 stanowisk) i SIEM do monitoringu stacji końcowych (poz. VII) – 1 szt.
3. **Miejski Ośrodek Pomocy Społecznej w Ciechocinku, ul. Mikołaja Kopernika 14, 87-720 Ciechocinek**
    1) Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ II (poz. I.2.) – 1 szt.

2) Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ II (poz. II.2) – 1 szt.

3) Wdrożenie usługi serwera logów systemowych i stacji końcowych oraz sieciowych (poz. III) – 1 szt.

4) Urządzenie typu NAS na potrzeby kopii wraz z instalacją i konfiguracją (poz. IV) – 1 szt.

5) Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (poz. VI) – system obejmujący 35 zasobów

6) Wdrożenie rozwiązań XDR (10 stanowisk) i SIEM do monitoringu stacji końcowych (poz. VII) – 1 szt.

4. **Szkoła Podstawowa nr 1 im. Marszałka Józefa Piłsudskiego w Ciechocinku, ul. Mikołaja Kopernika 18, 87-720 Ciechocinek**

1) Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ II (poz. I.2.) – 1 szt.

2) Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ I (poz. II.1) – 1 szt.

3) Wdrożenie usługi serwera logów systemowych i stacji końcowych oraz sieciowych (poz. III) – 1 szt

4) Urządzenie typu NAS na potrzeby kopii wraz z instalacją i konfiguracją (poz. IV) – 1 szt.

5) Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (poz. VI) – system obejmujący 85 zasobów

6) Wdrożenie rozwiązań XDR (10 stanowisk) i SIEM do monitoringu stacji końcowych (poz. VII) – 1 szt.

5. **Szkoła Podstawowa nr 3 im. Polskich Olimpijczyków w Ciechocinku, ul. Wojska Polskiego 37, 87-720 Ciechocinek**

1) Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ II (poz. I.2.) – 1 szt.

2) Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ III (poz. II.3) – 1 szt.

3) Wdrożenie usługi serwera logów systemowych i stacji końcowych oraz sieciowych (poz. III) – 1 szt

4) Urządzenie typu NAS na potrzeby kopii wraz z instalacją i konfiguracją (poz. IV) – 1 szt.

5) Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (poz. VI) – system obejmujący 50 zasobów

6) Wdrożenie rozwiązań XDR (10 stanowisk) i SIEM do monitoringu stacji końcowych (poz. VII) – 1 szt.

6. **Przedszkole Samorządowe nr 1 Bajka w Ciechocinku, ul. Widok 9, 87-720 Ciechocinek**

1) Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ II (poz. I.1.) – 1 szt.

2) Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ II (poz. II.2) – 1 szt.

3) Wdrożenie usługi serwera logów systemowych i stacji końcowych oraz sieciowych (poz. III) – 1 szt

4) Urządzenie typu NAS na potrzeby kopii wraz z instalacją i konfiguracją (poz. IV) – 1 szt.

5) Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (poz. VI) – system obejmujący 20 zasobów

6) Wdrożenie rozwiązań XDR (5 stanowisk) i SIEM do monitoringu stacji końcowych (poz. VII) – 1 szt.

7. **Przedszkole Samorządowe nr 2 im. Kubusia Puchatka w Ciechocinku, ul. Wierzbowa 10, 87-720 Ciechocinek**

1) Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ II (poz. I.1.) – 1 szt.

2) Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ II (poz. II.2) – 1 szt.

3) Wdrożenie usługi serwera logów systemowych i stacji końcowych oraz sieciowych (poz. III) – 1 szt

4) Urządzenie typu NAS na potrzeby kopii wraz z instalacją i konfiguracją (poz. IV) – 1 szt.

5) Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (poz. VI) – system obejmujący 20 zasobów

6) Wdrożenie rozwiązań XDR (5 stanowisk) i SIEM do monitoringu stacji końcowych (poz. VII) – 1 szt.

8. **Żłobek Samorządowy „Bajeczka" w Ciechocinku, ul. Widok 9, 87-720 Ciechocinek**

1) Urządzenie UTM wraz z licencjami, wsparciem i konfiguracją – typ II (poz. I.1.) – 1 szt.

2) Urządzenie typu serwer do gromadzenia logów sieciowych i systemowych wraz z instalacją – typ II (poz. II.2) – 1 szt.

3) Wdrożenie usługi serwera logów systemowych i stacji końcowych oraz sieciowych (poz. III) – 1 szt

4) Zakup urządzenia typu NAS na potrzeby kopii wraz z instalacją i konfiguracją (poz. IV) – 1 szt.

5) Wdrożenie systemu klasy SAM do gromadzenia informacji o oprogramowaniu i sprzęcie jednostek komputerowych, drukarek i sieci (poz. VI) – system obejmujący 20 zasobów

6) Wdrożenie rozwiązań XDR (5 stanowisk) i SIEM do monitoringu stacji końcowych (poz. VII) – 1 szt.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 5 do SWZ

.....
(miejscowość i data)

Wykaz dostaw

Działając w imieniu i na rzecz Wykonawcy, tj. .....
(pełna nazwa i adres wykonawcy/wykonawców w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia), w postępowaniu o udzielenie zamówienia publicznego pn. ,, Dostawa sprzętu i oprogramowania dla Gminy Miejskiej Ciechocinek" w celu potwierdzenia spełnienia warunku udziału w postępowaniu określonego w SWZ w zakresie zdolności zawodowej (doświadczenie) przedstawiam następujące dostawy:

Lp.	Nazwa i adres podmiotu na rzecz którego realizowane były dostawy	Nazwa zadania inwestycyjnego	Termin realizacji	Wartość brutto dostaw
1				
2				
3				

Jeżeli Wykonawca powołuje się na doświadczenie w realizacji dostaw, wykonywanych wspólnie z innymi wykonawcami, wykaz dotyczy dostaw, w których wykonaniu wykonawca ten bezpośrednio uczestniczył, w przypadku świadczeń powtarzających się lub ciągłych, w których bezpośrednio uczestniczył lub uczestniczy.

W celu potwierdzenia, że dostawy wskazane w powyższej tabeli zostały wykonane/ są wykonywane należycie załączam/-y do wykazu następujące dowody:

1. ..... - dowód do dostawy z poz. ....
2. ..... - dowód do dostawy z poz. ....
3. ..... - dowód do dostawy z poz. ....

Dokument należy opatrzyć
kwalifikowanym podpisem elektronicznym
lub podpisem zaufanym
albo podpisem osobistym

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 7 do SWZ

KARTA GWARANCYJNA

WYKONAWCA jako GWARANT: Firma:

ADRES:

Telefon: ....., e – mail: .....FAX:..... udziela gwarancji na cały zakres produktów/asortymentu objętego przedmiotem Umowy nr ..... z dnia ..... zawartą z ZAMAWIAJĄCYM – Gminą Miejską Ciechocinek , ul. Mikołaja Kopernika 19; 87-720 Ciechocinek w ramach postępowania pn.: **„Dostawa sprzętu i oprogramowania dla Gminy Ciechocinek"**

§1

Przedmiot gwarancji

1. Przedmiotem gwarancji jest nowy, wolny od wad fizycznych i prawnych dostarczone sprzęty z oprogramowaniem, zgodnie z poniższym zestawieniem:

Lp.	nazwa urządzenia/oprogramowania	model/typ	nr seryjny	producent	okres gwarancji
1					
2					
3					
4					
5					
6					
7					
8					
9					

Uwaga: Okres gwarancji liczony jest od daty podpisania protokołu odbioru końcowego.

§2

Zakres gwarancji

1. Gwarancja obejmuje w szczególności:

1) wady materiałowe i produkcyjne,

2) nieprawidłowe działanie lub uszkodzenia powstałe przy prawidłowym użytkowaniu zgodnie z przeznaczeniem,

2. Wykonawca zobowiązuje się do:

1) bezpłatnego usunięcia usterek i wad sprzętu wynikłych z przyczyn tkwiących w sprzęcie

2) zapewnienia części zamiennych niezbędnych do naprawy

3) czasu reakcji na zgłoszenie nie dłuższego niż 48h godzin liczonych od terminu zgłoszenia

4) naprawy lub wymiany sprzętu na nowy w przypadku niemożności usunięcia wady w terminie do 14 dni roboczych od daty zgłoszenia

5) wymiany wadliwych urządzeń lub/i poszczególnych komponentów na nowe, wolne od wad, jeżeli ten sam egzemplarz sprzętu lub/i komponent sprzętu były naprawiane w ramach gwarancji trzykrotnie.

6) W przypadku stwierdzenia wady ukrytej sprzętu Wykonawca zobowiązany jest do jego wymiany na nowy zgodnie z warunkami przedstawionymi w Opisie przedmiotu zamówienia.

3. Gwarancja nie obejmuje:

1) uszkodzeń mechanicznych powstałych z winy użytkownika,

2) uszkodzeń wynikłych z nieprawidłowego użytkowania niezgodnego z przeznaczeniem,

3) eksploatacyjnego zużycia materiałów

4) nieautoryzowanych napraw lub przeróbek sprzętu

4. W celu skorzystania z gwarancji Zamawiający zobowiązany jest do niezwłocznego zgłoszenia wady na piśmie lub drogą mailową.

§3

Komunikacja

1. Wszelka komunikacja pomiędzy stronami wymaga potwierdzenia w formie pisemnej. O każdej wadzie osoba wyznaczona przez ZAMAWIAJĄCEGO powiadamia telefonicznie przedstawiciela Gwaranta, a następnie potwierdza zgłoszenie telefaksem bądź e-mailem na wskazane numery telefonów i adresy. Kopia potwierdzenia zgłoszenia przesyłana jest również faksem lub e-mailem do ZAMAWIAJĄCEGO.

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 7 do SWZ

2. Pisma skierowane do GWARANTA należy wysyłać na adres :
3. Pisma skierowane do ZAMAWIAJĄCEGO należy wysyłać na adres: Urząd Gminy Ciechocinek, ul. Mikołaja Kopernika 19; 87-720 Ciechocinek
4. O zmianach danych teleadresowych strony obowiązane informować się niezwłocznie, nie później niż 7 dni od chwili zaistnienia zmian, pod rygorem uznania wysyłania korespondencji pod ostatnio znany adres za skutecznie doręczoną.

§4

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Karty Gwarancyjnej wymagają formy pisemnej pod rygorem nieważności
2. Niniejsza Karta Gwarancyjna stanowi załącznik nr 3 do Umowy nr ..... z dnia ..... r.
3. Podpisując niniejszą kartę gwarancyjną, Wykonawca oświadcza, że dostarczony sprzęt jest wolny od wad fizycznych i prawnych oraz objęty gwarancją na warunkach określonych powyżej.

.....

Podpis Wykonawcy

(data i miejsce)

.....

Podpis Zamawiającego

(data i miejsce)

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 8 do SWZ

Klauzula informacyjna FERC

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

Administrator danych

Odrębnymi administratorami Państwa danych są:

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

Cel przetwarzania danych

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

Podstawa przetwarzania

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

1. Zobowiązuje nas do tego prawo (art. 6 ust. 1 lit. c RODO):
   1) art. 87 ustawy wdrożeniowej,
   2) art. 61 ustawy z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r. poz. 1079),
   3) ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (tekst jednolity Dz.U. z 2023 r. poz. 775 z późn. zm.),
   4) art. 206 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity Dz. U. z 2022 r. poz. 1634, z późn. zm.),

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 8 do SWZ

5) Porozumienie trójstronne w sprawie systemu realizacji programu „Fundusze
6) rozporządzenia Ministra Cyfryzacji z dnia 16 lutego 2023 r. w sprawie udzielania pomocy na rozwój infrastruktury szerokopasmowej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (Dz. U. z 2023 r. poz. 405), Europejskie na Rozwój Cyfrowy 2021-2027" z 2.02.2023 r.,

2. Wykonujemy zadania w interesie publicznym lub sprawujemy powierzoną nam władzę publiczną (art. 6 ust. 1 lit. e RODO),
3. Przygotowujemy i realizujemy **umowy**, których są Państwo stroną, a przetwarzanie danych osobowych jest niezbędne do ich zawarcia i wykonania (art. 6 ust. 1 lit. b RODO).

Rodzaje przetwarzanych danych

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

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

Dostęp do danych osobowych

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

1. podmiotom, w tym ekspertom, o których mowa w art. 80 ustawy wdrożeniowej, którym zleciliśmy wykonywanie zadań w ramach realizacji FERC,
2. instytucji audytowej, o której mowa w art. 71 rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 8 do SWZ

Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej,

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

Okres przechowywania danych

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

Prawa osób, których dane dotyczą

Przysługują Państwu następujące prawa:

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

Zautomatyzowane podejmowanie decyzji

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

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 8 do SWZ

Przekazywanie danych do państwa trzeciego

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

Kontakt z administratorem danych i Inspektorem Ochrony Danych

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

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

Podstawa prawna:

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

Oznaczenie postępowania: BSR-ZP.271.3.2026

Załącznik nr 9 do SWZ

.....
(miejscowość i data)

Wykaz osób

Działając w imieniu i na rzecz Wykonawcy, tj. .....
(pełna nazwa i adres wykonawcy/wykonawców w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia), w postępowaniu o udzielenie zamówienia publicznego pn. ,, Dostawa sprzętu i oprogramowania dla Gminy Miejskiej Ciechocinek" w celu potwierdzenia spełnienia warunku udziału w postępowaniu określonego w SWZ w zakresie zdolności zawodowej (doświadczenie) przedstawiam następujące dostawy:

Lp.	Imię i nazwisko osoby wskazanej do realizacji zamówienia	Posiadane doświadczenie, uprawnienie niezbędne do wykazania spełnienia warunku udziału w postępowaniu	Podstawa dysponowania osobą/ jeżeli Wykonawca korzysta z zasobów podmiotu trzeciego zobowiązany jest określić podmiot udostępniający zasoby
1 (jedną) osobą, która będzie uczestniczyć w wykonywaniu zamówienia, posiadającą kwalifikacje, potwierdzone ważnym certyfikatem producenta oferowanego rozwiązania w zakresie oferowanych urządzeń klasy UTM, na poziomie co najmniej profesjonalnym (Professional) lub równoważnym, uprawniającym do samodzielnej instalacji, konfiguracji oraz utrzymania urządzeń. Certyfikat musi być ważny (aktywny) co najmniej na dzień składania ofert oraz musi zachować ważność przez cały okres realizacji zamówienia.			
1			
2			

Oświadczamy, że osoby umieszczone w niniejszym wykazie zostaną skierowane do realizacji zamówienia.

W celu potwierdzenia, że osoby wskazane w powyższej tabeli posiadają niezbędne kwalifikacje załączam/-y do wykazu następujące dowody:

1. ..... - dowód do dostawy z poz. ....
2. ..... - dowód do dostawy z poz. ....

Dokument należy opatrzyć
kwalifikowanym podpisem elektronicznym
lub podpisem zaufanym
albo podpisem osobistym