Sprawa: BDG-WII.262.14.2022 Warszawa, dnia 6 kwietnia 2022 r.

Wykonawcy

ZAPYTANIE DOTYCZĄCE OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo Edukacji i Nauki (MEiN), ul. Wspólna 1/3, 00-529 Warszawa (NIP: 7011010460, REGON: 387796051) zwraca się z zapytaniem dotyczącym dokonania oszacowania wartości zamówienia pn. ***Oprogramowanie dla Ministerstwa Edukacji i Nauki.***

1. PRZEDMIOT WYCENY

Część I

Przedłużenie wsparcia na posiadane przez Zamawiającego licencje wraz ze sprzętem na system Antyspamowy Symantec Messaging Gateway na 3 kolejne lata od dnia 02.11.2022 r.

Część II

1. Zakup wieczystej licencji typu Academic dla MS Exchange 2019 Standard (3 licencje) wraz z MS Exchange Server Standard 2019 User CAL (450 licencji) z możliwością upgrade do nowszej wersji przez okres 3 lat.
2. Zakup wieczystej licencji typu Academic dla Microsoft Office Standard 2021 - (dla 500 użytkowników).
3. Zakup wieczystej licencji typu Academic dla MS Windows Server Datacenter 2022 (na 176 core).
4. Zakup wieczystej licencji typu Academic dla MS Windows Server user CAL dla 500 użytkowników.
5. Zakup wieczystej licencji typu Academic dla MS Windows Server Standard 2022 (na 56 core).
6. Zakup wieczystej licencji typu Academic dla Windows Server 2022 RDS User CAL – (140 szt.).
7. Szkolenia dla zaoferowanych Systemów.

Część III

Przedłużenie posiadanych licencji ADSelf Service Professional na 3 kolejne lata od dnia 07.12.2022 r. – 500 licencji.

Część IV

Przedłużenie wsparcia na posiadane przez Zamawiającego licencje wraz ze sprzętem na system Kemp Loadbalancer na 3 kolejne lata od dnia 10.09.2022 r.

Część V

Przedłużenie wsparcia na posiadane przez Zamawiającego licencje dla systemu Archiwizacji poczty dla MS Exchange na 3 kolejne lata od dnia 11.09.2022 r.

Część VI

Przedłużenie wsparcia na posiadane licencje na system typu SIEM na 3 kolejne lata od dnia 18.12.2022 r.

Szczegółowy opis przedmiotu zamówienia został zawarty w *Załączniku nr 1* do zapytania o wycenę.

2. TERMIN ZŁOŻENIA WYCENY

Wycenę (wybraną część/części zamówienia), sporządzoną na Formularzu będącym *Załącznikiem nr 2* do zapytania o wycenę, proszę przesłać na adres oferty@mein.gov.pl **do dnia 20 kwietnia 2022 r.** (w tytule wiadomości proszę wpisać: „WYCENA – Oprogramowanie dla MEiN".

Ewentualne pytania dotyczące przedmiotowej wyceny proszę kierować na adres oferty@mein.gov.pl**.**

Łukasz Teterycz
Zastępca Dyrektora
Biura Dyrektora Generalnego
/ -podpisano kwalifikowanym podpisem elektronicznym /

Załacznik nr 1 do zapytania o wycenę

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA w zakresie części I, II, III, IV, V, VI

Część I przedmiotu zamówienia

lp.	*nazwa licencji/ oprogramowania*
Przedłużenie wsparcia na posiadane przez Zamawiającego licencje wraz ze sprzętem na system Antyspamowy Symantec Messaging Gateway na 3 kolejne lata od dnia 02.11.2022 r.:	
a) Messaging Gateway 8340 Appliance. b) End Customer SMG Support, Next Business Day Delivery Hardware Support – wsparcie dla appliance 2 szt. c) Messaging Gateway Initial Subscription License with Support ACD-GIV 500-999 User 3TR – 800 szt.	
Równoważny system musi mieć co najmniej funkcjonalności: 1. System musi posiadać zintegrowane rozwiązania antywirusowe, antyspamowe i filtrowania treści. 2. System musi umożliwiać pracę w trybie bramki pocztowej. 3. System musi umożliwiać blokowanie spamu w oparciu o lokalne polityki, silnik skanujący i bazy. Poczta w żadnym przypadku nie jest przekierowywana na serwery usługodawcy. 4. Rozwiązanie antyspamowe musi posiadać skuteczność powyżej 98% i równocześnie charakteryzować się współczynnikiem fałszywych alarmów na poziomie 1 na milion, co zostało potwierdzone przez niezależne testy. 5. Do wykrywania spamu, system musi wykorzystywać bazy z numerami IP lub nazwami domen spamerów. 6. System musi zapewniać routing wiadomości pocztowych w oparciu o domenę i adres odbiorcy. 7. System musi umożliwiać zmianę domeny i nazwy użytkownika w wiadomości przychodzącej i wychodzącej dla odbiorcy i nadawcy odpowiednio dla ruchu przychodzącego i wychodzącego. 8. System musi umożliwiać tworzenie aliasów dla grup użytkowników. 9. System musi zapewniać dopisywanie domyślnej nazwy domeny dla nadawcy wiadomości. 10. System musi zapewniać ochronę przed skanowaniem serwera pocztowego w poszukiwaniu istniejących (prawidłowych) adresów pocztowych. 11. System musi zapewniać usuwanie nagłówków Received z wysyłanych wiadomości. 12. Wiadomości z systemów próbujących atakować spamem serwer pocztowy, muszą być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako spam z jednego adresu IP lub jednego nadawcy w danym przedziale czasu).	

13. Wiadomości z systemów próbujących atakować wirusami serwer pocztowy, muszą być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako wirusy z jednego adresu IP lub jednego nadawcy w danym przedziale czasu).
14. Połączenia z systemów próbujących atakować spamem serwer pocztowy, muszą być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako spam z jednego IP w danym przedziale czasu).
15. Administrator musi mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie zawsze dozwolona i nie będzie blokowana przez żaden silnik.
16. Administrator musi mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie zawsze blokowana.
17. System musi posiadać niezależnie konfigurowane polityki dla wiadomości przychodzących i wychodzących.
18. System musi posiadać funkcję ograniczającą dostępne pasmo dla maszyn/domen przesyłających spam, ale nieblokująca w całości komunikacji z tymi maszynami/domenami.
19. Aktualizacje sygnatur spamu nie rzadziej, niż co 1 min.
20. Aktualizacje sygnatur antywirusowych nie rzadziej, niż co 1 godzina.
21. Rozwiązanie antywirusowe musi kasować skompresowane załączniki do 10 poziomów zagnieżdżeń i być odporne na złośliwie spreparowane załączniki („załączniki bomby”).
22. Wiadomości z wirusami typu mass-mailer muszą być w całości odrzucane, bez podejmowania dodatkowych akcji, takich jak np. powiadomienie.
23. System musi umożliwiać znakowanie załączników dla odróżnienia ich treści.
24. System musi wykrywać fałszywe URL-e w wiadomościach.
25. System musi umożliwiać analizę html mającą na celu przeciwdziałanie metodom utrudniającym analizę treści wiadomości (np.: losowo generowane ciągi, nieprawidłowe kody formatujące).
26. System musi umożliwiać detekcję języka, w którym została napisana wiadomość i mieć możliwość użycia tej informacji, jako kryterium przy przetwarzaniu wiadomości.
27. System musi umożliwiać kontrolę treści w oparciu o słowa kluczowe lub słowniki definiowane przez administratora, w tym sprawdzanie zawartości skompresowanych archiwów.
28. System musi posiadać mechanizmy tworzenia reguł kontroli treści, wiązanie wymagań przy pomocy logicznych „I” i „LUB”, możliwość budowania reguł w postaci negatywnej „NIE”.
29. System musi mieć możliwość dodawania do wysyłanych wiadomości zdefiniowanego tekstu.
30. System musi umożliwiać nakładania polityk na załączniki w oparciu o ich rozmiar, typ MIME, nazwę pliku lub jego rozszerzenie – w tym identyfikację prawdziwego rozszerzenia pliku.
31. System musi umożliwiać wykonanie następujących akcji przy wiadomościach sklasyfikowanych jako spam:
    1) usunięcie;

2) dodanie nagłówka wiadomości;
3) modyfikacja – dodanie informacji dla odbiorcy;
4) zarchwizowanie czyli wysłanie kopii oryginalnej wiadomości na dedykowany serwer;
5) BCC – wysłanie blind carbon copy na inny adres pocztowy;
6) Bounce – odpowiedź do nadawcy wiadomością z modyfikowalnym NDR;
7) wyczyszczenie, jeśli wiadomość zawierała wirusa;
8) dostarczenie bez modyfikacji;
9) przekierowanie na inny adres pocztowy;
10) zmodyfikowanie tematu wiadomości,
11) wrzucenie wiadomości do centralnej kwarantanny;
12) przesłanie powiadomienia na wybrany adres;
13) usunięcie załącznika z wiadomości;
14) wysłanie wiadomości spam niewykrytych przez rozwiązanie do producenta, w celu ich analizy.

32. System musi kategoryzować wiadomości przynajmniej na:
1) normalne wiadomości bez spamu i wirusów;
2) spam;
3) podejrzane o spam;
4) biuletyn (tzw. newsletter);
5) wiadomość marketingowa;
6) wiadomość z podejrzanym adresem URL;
7) wirusy masowe;
8) wiadomości zawierające wirusy;
9) wiadomości, których nie można przeskanować;
10) wiadomości od blokowanych nadawców;
11) wiadomości zablokowane na podstawie filtrów przygotowanych przez administratora.

33. System musi mieć wsparcie dla Transport Layer Security (TLS) – definiowane per domena lub polityka, Sender Policy Framework (SPF), Sender ID.
34. System musi mieć możliwość importowania bazy użytkowników poprzez LDAP.
35. System musi umożliwiać administratorowi ingerencję w czułości wykrywania.
36. Rozwiązanie musi posiadać serwer kwarantanny. Serwer musi być dostępny dla poszczególnych użytkowników końcowych. Serwer musi przesyłać okresowe powiadomienia o zawartości kwarantanny. Powiadomienia muszą mieć wbudowane mechanizmy do zarządzania zawartością kwarantanny (przesłanie dalej, podgląd, zalogowanie do kwarantanny).
37. Na serwer kwarantanny musi być możliwość nałożenia ograniczenia dla poszczególnych użytkowników jak i całego serwera wg ilości przechowywanych wiadomości, ilości zajętego miejsca itp..

38. Komunikacja pobierania uaktualnień musi być szyfrowana.
39. Komunikacja umożliwiająca zarządzanie systemem musi być szyfrowana.
40. Rozwiązanie musi być centralnie zarządzane z wbudowanymi mechanizmami raportowania. Jedna konsola musi umożliwiać zarządzanie kilkoma współpracującymi urządzeniami. Wykonywane raporty muszą uwzględniać dane zebrane ze wszystkich współpracujących urządzeń.
41. System musi posiadać min. 50 wbudowanych raportów. Wykonanie raportów można zaplanować w dzienniku. Gotowe raporty można przesłać do skrzynki pocztowej wyznaczonych odbiorców.
42. System musi umożliwiać tworzenie wielu kont administracyjnych z różnymi poziomami uprawnień, w tym możliwość zdefiniowania użytkowników mających dostęp do różnych kwarantann.
43. System musi umożliwiać definiowanie poziomu logowania o swojej aktywności.
44. System musi powiadamiać wybranych administratorów o nieprawidłowej pracy komponentów.
45. System musi umożliwiać wykonywanie zaplanowanych kopii bezpieczeństwa konfiguracji i baz kwarantanny oraz możliwość odtworzenia konfiguracji z tak wykonanej kopii.
46. System musi posiadać zestaw poleceń dostępny z konsoli systemu operacyjnego.
47. System musi umożliwiać graficzne śledzenie wiadomości, w tym informacje, co stało się z wiadomością.
48. System musi posiadać wewnętrzną bazę reputacji, śledzącą adresy IP serwerów pocztowych.
49. System musi umożliwiać zapytanie o adres IP do wewnętrznej i globalnej bazy reputacji.
50. System musi umożliwiać stworzenie odpowiednio obsługiwanych kolejek z punktu widzenia reputacji danego adresu IP – ograniczając taki adres do ilości wysyłanych wiadomości, ilości nawiązywanych połączeń w określonym czasie.
51. System musi mieć możliwość zdefiniowania osobnej kwarantanny dla poczty naruszającej reguły zgodności z polityką określającą rodzaj przesyłanych treści.
52. System musi umożliwiać skorzystanie z predefiniowanych polityk i wzorców.
53. System musi umożliwiać rozpatrywanie incydentów skojarzonych z naruszeniem polityk, w tym definiowanie ważności incydentu.
54. Rozpatrując incydent z góry muszą być określone akcje, które osoba rozpatrująca incydent może podjąć, np. rozpoczęcie śledztwa, przesłanie widomości do odbiorcy, przesłanie wiadomości do nadawcy, itp.,
55. System musi posiadać ochronę przed atakami wirusów typu Day Zero oraz zdefiniowaną kwarantannę dla złapanych w ten sposób wirusów z możliwością ustawienia czasu, przez który zatrzymane maile mają w niej pozostawać.

56. System musi umożliwiać wysyłkę źle sklasyfikowanych wiadomości typu spam do producenta, gdzie automatycznie zostaną przygotowane sygnatury antyspamowe i natychmiast dostarczone do rozwiązania.
57. System musi posiadać możliwość wysyłania alertów SNMP.
58. System musi wspierać autentykację DomainKeys Identified Mail (DKIM).
59. System musi wspierać autentykację DMARC.
60. System musi wspierać autentykację SMTP.
61. System musi wykorzystywać Bounce Attack Tag Validation (BATV).
62. Wszystkie aspekty konfiguracyjne związane z SPF, DKIM i DMARK muszą być konfigurowane przez przeglądarkę WEB. Ze względów bezpieczeństwa nie mogą mieć możliwości ręcznej konfiguracji na plikach tekstowym na urządzeniu (np. poprzez ręczną zmianę informacji w plikach konfiguracyjnych usług pocztowych).
63. System musi zapewniać dedykowaną ochronę dla potencjalnie niebezpiecznej zawartości (makra, skrypty, osadzony Flash, itp.) znajdującej się w plikach PDF oraz plikach pakietu Microsoft Office, polegającą na przebudowaniu takiego dokumentu, usuwając z niego potencjalnie niebezpieczną zawartość według określonego kryterium – np.: usuwaj Flash, pozostaw makra.

Część II przedmiotu zamówienia

lp.	*nazwa licencji/ oprogramowania*
1	**Zakup wieczystej licencji typu Academic dla MS Exchange 2019 Standard (3 licencje) wraz z MS Exchange Server Standard 2019 User CAL (500 licencji) z możliwością upgrade do nowszej wersji przez okres 3 lat**

Wykonawca zapewni dostęp do spersonalizowanej strony Producenta ze zdefiniowanym Kontem Zakupowym Zamawiającego pozwalającym upoważnionym osobom ze strony Zamawiającego na:

a) Pobieranie zakupionego oprogramowania,
b) Sprawdzanie liczby aktywacji w wykazie zakupionych produktów.

Warunki równoważności serwerowego systemu poczty elektronicznej (licencja na serwer):

Serwer poczty elektronicznej musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:
   1) odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych;
   2) mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata;
   3) tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami;

4) zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia;
5) wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości;
6) pełne wsparcie dla klienta poczty elektronicznej MS Outlook 2016 i nowszych wersji.

2. Funkcjonalność wspierająca pracę grupową:
1) możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie;
2) możliwość określenia terminu wygaśnięcia wiadomości;
3) udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu;
4) podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze;
5) mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone;
6) mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania;
7) tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań;
8) mechanizm udostępniania współdzielonych skrzynek pocztowych;
9) obsługa list i grup dystrybucyjnych;
10) dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów;
11) możliwość informowania zewnętrznych użytkowników poczty elektronicznej o dostępności lub niedostępności;
12) możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności;
13) widok rozmowy, automatycznie organizujący wątki wiadomości w oparciu o przebieg wymiany wiadomości między stronami;
14) konfigurowalna funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności;
15) udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby wsparcia ze strony informatyków;
16) mechanizm automatycznego dostosowywania się funkcji wyszukiwania kontaktów do najczęstszych działań użytkownika skutkujący priorytetyzacją wyników wyszukiwania;

17) możliwość wyszukiwania i łączenia danych (zgodnie z nadanymi uprawnieniami) z systemu poczty elektronicznej oraz innych systemów w organizacji (portali wielofunkcyjnych, komunikacji wielokanałowej i serwerów plików);

18) Możliwość dostępu do poczty elektronicznej i dokumentów przechowywanych w portalu wielofunkcyjnym z poziomu jednego interfejsu zarządzanego przez serwer poczty elektronicznej.

3. Funkcjonalność wspierająca zarządzanie systemem poczty:
   1) oparcie się o profile użytkowników usługi katalogowej Active Directory;
   2) wielofunkcyjna konsola administracyjna umożliwiająca zarządzanie systemem poczty oraz dostęp do statystyk i logów użytkowników;
   3) definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu;
   4) możliwość definiowania różnych limitów pojemności skrzynek dla różnych grup użytkowników;
   5) możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer;
   6) możliwość korzystania z interfejsu internetowego w celu wykonywania częstych zadań związanych z pomocą techniczną;
   7) narzędzia kreowania, wdrażania i zarządzania politykami nazewnictwa grup dystrybucyjnych.
4. Utrzymanie bezpieczeństwa informacji:
   1) centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym: śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, oraz archiwizacja danych;
   2) możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych;
   3) mechanizm zapobiegania wycieku danych ograniczający możliwość wysyłania danych poufnych do nieuprawnionych osób poprzez konfigurowalne funkcje monitoringu i analizy treści, bazujący na ustalonych politykach bezpieczeństwa;
   4) możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości;
   5) możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez osoby odpowiedzialne za zgodność z uregulowaniami;

6) integracja z usługami zarządzania dostępem do treści pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania. Wymagana jest możliwość użycia 2048-bitowych kluczy RSA, 256-bitowych kluczy SHA-1 oraz algorytmu SHA-2;
7) odbieranie wiadomości zabezpieczonych funkcją IRM przez zewnętrznych użytkowników oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS;
8) przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji;
9) wbudowane filtrowanie oprogramowania złośliwego, wirusów i oprogramowania szpiegującego zawartego w wiadomościach wraz z konfigurowalnymi mechanizmami powiadamiania o wykryciu i usunięciu takiego oprogramowania;
10) mechanizm audytu dostępu do skrzynek pocztowych z kreowaniem raportów audytowych.

5. Wsparcie dla użytkowników mobilnych:
1) możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu. Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem;
2) możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.);
3) możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone;
4) możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej;
5) umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Mozilla Firefox, Google Chrome, Microsoft Edge;

6. Funkcje związane z niezawodnością systemu:
1) zapewnienie pełnej redundancji serwerów poczty elektronicznej bez konieczności wdrażania klastrów oraz niezależnych produktów do replikacji danych;
2) automatyzacja replikacji bazy danych i przełączania awaryjnego już dla dwóch serwerów poczty, a także w wypadku centrów danych rozproszonych geograficznie;

3) utrzymanie dostępności i uzyskanie możliwości szybkiego odzyskiwania po awarii dzięki możliwości konfiguracji wielu replik każdej bazy danych skrzynki pocztowej;
4) automatyczne odtwarzanie redundancji poprzez tworzenie kopii zapasowych w miejsce kopii na uszkodzonych dyskach według zadanego schematu;
5) ograniczenie zakłócenia pracy użytkowników podczas przenoszenia skrzynek pocztowych między serwerami, pozwalające na przeprowadzanie migracji i konserwacji w dowolnym czasie – nawet w godzinach pracy biurowej;
6) zapewnienie ochrony przed utratą e-maili spowodowaną uaktualnianiem lub awarią roli serwera transportu poprzez zapewnienie redundancji i inteligentne przekierowywanie poczty na inną dostępną ścieżkę.

2	**Zakup wieczystej licencji typu Academic dla Microsoft Office Standard 2021 - (dla 500 użytkowników)**

Oferowane rozwiązanie równoważne dla Microsoft Office Standard 2021 musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1) Wykonawca zapewni dostęp do spersonalizowanej strony Producenta ze zdefiniowanym Kontem Zakupowym Zamawiającego pozwalającym upoważnionym osobom ze strony Zamawiającego na:
   a) Pobieranie zakupionego oprogramowania,
   b) Sprawdzanie liczby aktywacji w wykazie zakupionych produktów.
2) Dostępność pakietu w wersji 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.
3) Wymagania odnośnie interfejsu użytkownika:
   a) Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski,
   b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych,
   c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
4) Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
5) Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu Microsoft Office i badania zgodności z dokumentami wytworzonymi w tym pakiecie.
6) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:

a) posiada kompletny i publicznie dostępny opis formatu,
b) ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 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. 2012, poz. 526),
c) umożliwia kreowanie plików w formacie XML,
d) wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,

7) Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz poprawnie współpracować z dodatkiem AddIn do Systemu EZD PUW (ezd.gov.pl).
8) Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
9) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
10) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
11) Pakiet zintegrowanych aplikacji biurowych musi zawierać:
    a) Edytor tekstów,
    b) Arkusz kalkulacyjny,
    c) Narzędzie do przygotowywania i prowadzenia prezentacji,
    d) Narzędzie do tworzenia drukowanych materiałów informacyjnych,
    e) Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
    f) Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
12) Edytor tekstów musi umożliwiać:
    a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b) Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c) Wstawianie oraz formatowanie tabel.
    d) Wstawianie oraz formatowanie obiektów graficznych.
    e) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    f) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    g) Automatyczne tworzenie spisów treści.
    h) Formatowanie nagłówków i stopek stron.

i) Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.

j) Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.

k) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.

l) Określenie układu strony (pionowa/pozioma).

m) Wydruk dokumentów.

n) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.

o) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.

p) Zapis i edycję plików w formacie PDF.

q) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

13) Arkusz kalkulacyjny musi umożliwiać:

a) Tworzenie raportów tabelarycznych.

b) Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.

c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.

d) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)

e) Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.

f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.

g) Wyszukiwanie i zamianę danych.

h) Wykonywanie analiz danych przy użyciu formatowania warunkowego.

i) Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS.

j) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.

k) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.

l) Formatowanie czasu, daty i wartości finansowych z polskim formatem.

m) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.

n) Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.

o) Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).

p) Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.

q) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

14) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

a) Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory,

b) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,

c) Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,

d) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,

e) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,

f) Automatyczne grupowanie poczty o tym samym tytule,

g) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,

h) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,

i) Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,

j) Zarządzanie kalendarzem,

k) Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,

l) Przeglądanie kalendarza innych użytkowników,

m) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,

n) Zarządzanie listą zadań,

o) Zlecanie zadań innym użytkownikom,

p) Zarządzanie listą kontaktów,

q) Udostępnianie listy kontaktów innym użytkownikom,

r) Przeglądanie listy kontaktów innych użytkowników,

s) Możliwość przesyłania kontaktów innym użytkowników,

t) Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

3	**Zakup wieczystej licencji typu Academic dla MS Windows Server Datacenter 2022 (na 176 core)**

Wykonawca zapewni dostęp do spersonalizowanej strony Producenta ze zdefiniowanym Kontem Zakupowym Zamawiającego pozwalającym upoważnionym osobom ze strony Zamawiającego na:

a) Pobieranie zakupionego oprogramowania,

b) Sprawdzanie liczby aktywacji w wykazie zakupionych produktów.

Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

1) Możliwość wykorzystania nielimitowanej liczby rdzeni logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64 TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z 64 węzłów.
4) Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywanych w bieżącej pracy.
7) 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).
8) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
9) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
10) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 11.
11) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
12) Możliwość wykorzystania standardu http/2.

13) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
15) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
16) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
17) Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
18) 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.
19) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
20) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
21) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
22) Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
23) Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
24) 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,
iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows

c. Zdalna dystrybucja oprogramowania na stacje robocze,
d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
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. Uruchamianie systemu typu Secure Boot uniemożliwiające modyfikacje wszystkich komponentów uruchomieniowych systemu (hardware root-of-trust),
h. Ochrona firmware sprzętowego przez system przed nieupoważnionym dostępem.
i. Mechanizmy umożliwiajcie ochronę wydzielonych obszarów pamięci przed dostępem bazujące na wirtualizacji sprzętowej.
j. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
k. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
l. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
m. Serwis udostępniania stron WWW z uruchomionym domyślnie TLS 1.3
n. Wsparcie dla protokołu IP w wersji 6 (IPv6),
o. Wsparcie dla algorytmów Suite B (RFC 4869),
p. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
q. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych,

r. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,

s. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności,

t. Mechanizmy wirtualizacji mające 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),

vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

25) Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.

26) Wsparcie dla rozwiązania Kubernetes.

27) 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.

28) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

29) Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.

30) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

31) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

32) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

33) Mechanizm konfiguracji połączenia VPN do platformy Azure.

34) Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.

35) Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.

36) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

4	**Zakup wieczystej licencji typu Academic dla MS Windows Server user CAL dla 500 użytkowników**

Opis równoważności dla Windows Server user CAL

Oprogramowanie równoważne musi zapewniać:

1) Prawo do dostępu do zakupionego serwera Windows DataCenter Server 2022 lub równoważnego, oraz posiadanych przez Zamawiającego serwerów rodziny Windows Server (2016 i 2019 standard) dla 500 użytkowników.
2) Każda z licencji musi zapewniać imienne przypisanie do jednego użytkownika.
3) Przeniesienie licencji między użytkownikami może odbyć się w okresie 90 dni (retencja licencji).
4) Licencja, wraz z dostarczonym pakietem tego samego producenta, zapewni dostęp do wszystkich funkcji Windows DataCenter Server 2022 oraz Windows Standard Server 2022.

5	**Zakup wieczystej licencji typu Academic dla MS Windows Server Standard 2022 (na 56 core)**

Wykonawca zapewni dostęp do spersonalizowanej strony Producenta ze zdefiniowanym Kontem Zakupowym Zamawiającego pozwalającym upoważnionym osobom ze strony Zamawiającego na:

a) Pobieranie zakupionego oprogramowania,

b) Sprawdzanie liczby aktywacji w wykazie zakupionych produktów.

Opis równoważności dla MS Windows Server Standard 2022 (wymagania minimalne dla równoważnego oprogramowania):

a. współpraca z procesorami o architekturze x86-64
b. instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym
c. w ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wyposażonym w 2 rdzenie
d. praca w roli serwera domeny Microsoft Active Directory
e. zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP)
f. zawarta możliwość uruchomienia roli serwera DNS
g. zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP)
h. zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
i. zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
j. zawarta możliwość uruchomienia roli serwera stron WWW

	k. w ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera l. w ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych m. wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
6	**Zakup wieczystej licencji typu Academic dla Windows Server 2022 RDS User CAL – (140 szt.)**
Opis wymagań dla Windows Server 2022 RDS User CAL (wymagania minimalne dla równoważnego oprogramowania): Licencja dostępowa dla użytkownika uprawniająca do korzystania z usługi pulpitu zdalnego na serwerach z systemem operacyjnym Windows Server 2022.	
7	**Szkolenia dla zaoferowanych Systemów:**
1. Wykonawca zapewni autoryzowane szkolenie w postaci 12 miesięcznych Voucher'ów (podstawowe i zaawansowane) dla 3 administratorów Zamawiającego, dotyczące zaoferowanych systemów (pkt. 1 i 3) - łącznie 12 szkoleń. 2. Plan i zakres szkoleń zostanie uzgodniony z Wykonawcą. 3. Łączny czas jednego szkolenia min. 40 godz.. 4. W trakcie szkolenia dla uczestników szkolenia w ciągu dnia musi być dostarczony przynajmniej jeden posiłek ciepły i dwie przerwy kawowe. 5. Szkolenie musi być przeprowadzone w formie, gdzie minimum 50% czasu szkolenia to będą warsztaty praktyczne. 6. Szkolenie musi być przeprowadzone w języku polskim. 7. Dla każdego uczestnika szkolenia muszą zostać dostarczone materiały szkoleniowe w postaci elektronicznej i przeszukiwalnej oraz umożliwiającej jednoczesne korzystanie z materiałów bez wykorzystywania komputera szkoleniowego- eliminacja konieczności przełączania się pomiędzy materiałami szkoleniowymi i środowiskiem szkoleniowym do ćwiczeń. Po zakończeniu szkolenia materiały szkoleniowe muszą zostać przekazane kursantom w tej samej postaci. 8. Szkolenie będzie realizowane w miejscu zaoferowanym przez Wykonawcę na terenie Warszawy.	

8	**Migracja MS Exchange 2016 do MS Exchange 2019 :**

Aktualizacja Microsoft Exchange 2016 do 2019 lub nowszy będzie wymagała między innymi:

1. Rozszerzenia schematu domeny na potrzeby systemu Microsoft Exchange 2019
2. Przeglądu środowiska Microsoft Exchange i weryfikacji poprawności jego działania
3. Przygotowania projektu technicznego migracji do akceptacji zamawiającego
4. Instalacji systemu Microsoft Exchange 2019 Standard na trzech maszynach wirtualnych
5. Konfiguracji środowiska klastra DAG zgodnie z projektem technicznym,
6. Koncepcji wykonania prac (jakie usługi i klienci, przepływ ruchu na styku Internet/DMZ/ /Exchange/LAN
7. Konfiguracji systemu Microsoft Exchange 2019,
8. Instalacji certyfikatu SSL w systemie Microsoft Exchange
9. Migracji usług oraz danych do nowego systemu,
10. Konfiguracji i weryfikacji poprawności działania replikacji pomiędzy lokalizacjami wykonawcy
11. Konfiguracji środowiska na potrzeby dostępu do usług z Internetu
12. Konfiguracji 2FA dla środowiska
13. Wygaszenia starego środowiska Exchange,
14. Stabilizacji środowiska i weryfikacja poprawności działania,
15. Testowania środowiska i sprawdzenia obiegu poczty w sieci lokalnej oraz u klientów mobilnych,
16. Weryfikacji podatności Serwerów Exchange oraz zabezpieczenie zgodnie z najlepszymi praktykami,
17. Stabilizacji środowiska i weryfikacja poprawności działania systemu poczty w tym sprawdzenie logów i poprawności pracy MS OS /Exchange, IIS
18. Konfiguracji Archiwizacji Poczty Veritas Enterprice Vault w celu archiwizacji skrzynek i journaling dla nowego środowiska MS Exchange 2019
19. Konfiguracji Backupu nowego środowiska MS Exchanga 2019 w środowisku Veritas NetBackup
20. Wykonania dokumentacji powykonawczej.

Część III przedmiotu zamówienia

lp.	*nazwa licencji/ oprogramowania*
Przedłużenie posiadanych licencji ADSelf Service Professional na 3 kolejne lata od dnia 07.12.2022 r. – 500 licencji	
Równoważny system musi mieć co najmniej funkcjonalności:	

1. Samoobsługa resetowania hasła,
2. Zarządzanie odblokowaniem konta,
3. Powiadomienie użytkowników o wygaśnięciu hasła/konta,
4. Jednokrotne logowanie przemysłowe,
5. Synchronizacja haseł,
6. Dwuetapowe uwierzytelnianie logowania Windows,
7. Aktualizowanie informacji osobistych w AD,
8. Mobilne zarządzanie hasłami,
9. Agent GINA/Mac/Linux (Ctrl+Alt+Del),
10. Uwierzytelnianie wieloskładnikowe,
11. Wymuszanie zasad haseł,
12. Dostosowywanie komputerów stacjonarnych i aplikacji mobilnych.

Część IV przedmiotu zamówienia

lp.	*nazwa licencji/ oprogramowania*
Przedłużenie wsparcia na posiadane przez Zamawiającego licencje wraz ze sprzętem na system Kemp Loadbalancer na 3 kolejne lata od dnia 10.09.2022 r.:	
a)	ENP-LM-X3 – 3 Year Enterprise Plus Subscription for LoadMaster LM-X3. Includes 7x24 Telephone & E-Mail Support Next Business Day Advanced Replacement Hardware Maintenance security notifications hotfixes software updates KEMP 360 Central management and automation KEMP
b)	LM-X3 LoadMaster LM-X3 hardware appl. lncludes 3.4 Gbps 1700 SSL TPS (2K keys) 8x1Gb Ports. Support Required – 2 szt.
Równoważny system musi mieć co najmniej funkcjonalności:	
1	Urządzenie(-a) muszą posiadać następujące parametry techniczne:
	1.1 Urządzenie do szafy rackowej nieprzekraczające wysokości 1U, wewnętrzna pamięć masowa o pojemności minimum 500 GB, pamięć RAM minimum 8 GB.
	1.2 Urządzenie musi być wyposażone w fizyczne interfejsy komunikacji: port konsoli (RJ-45); port VGA, minimum 8 portów Gigabit Ethernet.
	1.3 Terminowanie i obsługa ruchu szyfrowanego protokołem SSL.
	Wydajność obsługi ruchu TLS (SSL) przez jedną instancje, ilość nawiązywanych nowych transakcji SSL na sekundę z uwzględnieniem wariantów minimalnej długości klucza szyfrowania.
	- SSL TPS (2K Keys): 1,700
	1.4 Urządzenie musi zapewniać przepustowość minimum:
	- L4 3.6Gbs
	- L7 3.4Gbs

- obsługa minimum 69 000 transakcji http L7 na sekundę
- obsługa minimum 125 000 jednoczesnych połączeń L7.
- obsługa minimum 8 600 000 jednoczesnych połączeń L4.

1.5 Urządzenie musi wspierać tworzenie i zarządzanie Virtual LAN według standardu IEEE 802.1Q (agregacja Vlan, trunking).

1.6 Urządzenie musi wspierać Link Interface Bonding dla modeli: 802.3ad, link Failover.

1.7 Urządzenie musi umożliwiać równoważenie obciążenia ruchu TCP/UDP na serwerach rzeczywistych i wirtualnych.

1.8 Urządzenie musi umożliwiać terminowanie i akceleracje ruchu SSL w celu odciążenia serwerów rzeczywistych.

1.9 Urządzenie musi być wyposażone w zaawansowany system przeźroczystego buforowania dla protokołów HTTP/HTTPS.

1.10 Urządzenie musi umożliwiać kompresję treści dla statycznego ruchu HTTP/HTTPS.

2 Urządzenie(-a) muszą umożliwiać

2.1 Balansowanie ruchu L4/L7 dla serwerów polegające na tworzeniu wirtualnych adresów IP minimum 1000 VIP i ukrycia za nimi do 1000 serwerów.

2.2 Pracę w architekturze wysokiej dostępności w postaci klastra Active/Hot Standby w trybie gwarantowanej ciągłości pracy (Stateful Failover). Umożliwia komunikację klastra przez sieć Ethernet. Funkcjonalność uruchomienia klastra musi być dostarczona wraz z urządzeniem; jeśli wymaga to dodatkowych licencji to muszą być dostarczone wraz z produktem.

2.3 Urządzenie musi zapewniać możliwość przełączania ruchu dla warstwy 7 na podstawie treści „content switching" co najmniej w zakresie:

- Content Matching: Dopasuj zawartość nagłówka lub treści z zasadą/regułą
- Add Header: Dodaj nagłówek zgodnie z zasadą/regułą
- Del Header: Usuwj nagłówek zgodnie z zasadą/regułą
- Replace Header: Zastępuj nagłówek zgodnie z zasadą/regułą
- Modify URL: Zmieniaj adres URL zgodnie z zasadą/regułą

2.4 Urządzenie musi wykorzystywać przynajmniej następujące metody równoważenie ruchu:

- Round Robin (Cykliczny)
- Weighted Round Robin (Cykliczny ważony)
- Least Connection (Najmniejsza ilość połączeń)
- Weighted Least Connection (Ważona najmniejsza ilość połączeń)
- Agent-based Adaptive
- SDN Adaptive
- Chained Failover (Fixed Weighting)
- Source-IP Hash

- Layer 7 Content Switching
- AD Group based traffic steering

2.5 Urządzenie musi umożliwiać edytowanie i wdrażanie wirtualnych serwisów „w locie".

2.6 Urządzenie musi przeprowadzić auto rekonfiguracje w przypadku wykrycia awarii serwera rzeczywistego.

2.7 Przejście określonego ruchu tą samą drogą bazując na dowolnej informacji z nagłówka i zawartości pakietu IP.

2.8 Urządzenie musi umożliwiać sprawdzanie statusów serwerów poprzez internetowy protokół komunikatów kontrolnych.

2.9 Urządzenie musi wspierać konfigurację Direct Server Return.

2.10 Urządzenie musi umożliwiać konfigurację wsparcia dla topologii usług S-NAT.

2.11 Urządzenie musi być wyposażone w wbudowany system wykrywania sesji dla Microsoft Terminal Services.

2.12 Akceleracje SSL na urządzeniu musi umożliwiać wsparcie dla klucza RSA-2048bit.

2.13 Urządzenie musi mieć możliwość generowania zapytań CSR w celu potwierdzenia z centrum autoryzacyjnym zgodności certyfikatu. (CSR - Certificate Signing Request)

2.14 Urządzenie musi zapewniać bazę przechowywania i użycia co najmniej 256 certyfikatów TLS (SSL)

2.15 Urządzenie musi umożliwiać stosowanie certyfikatów firm trzecich.

2.16 Urządzenie musi oferować wsparcie dla certyfikatów typu extended validation oraz certyfikaty pośredniczące (Intermediate certificates).

2.17 Urządzenie musi zapewniać możliwość bezpiecznego zdalnego logowania dla administratorów poprzez SSH oraz HTTPS.

2.18 Urządzenie musi oferować pełną konfiguracje poprzez przeglądarkę internetową

2.19 Produkt musi oferować narzędzie do centralnego zarządzania load balancerami, monitorowania wydajności, scentralizowanych i zaplanowanych aktualizacji firmware, tworzenia backup'ów konfiguracji, zaplanowania reboot load balancera, pobrania log'ów systemowych.

2.20 Produkt musi oferować wsparcie dla protokołu IPv6 oraz konwersji IPv4 <-> IPv6

2.21 Urządzenie musi wyświetlać w czasie rzeczywistym informacje o dostępności i wydajności. Wymagana obsługa protokołów monitorowania SYSLOG, SNMP, in-line TCP-DUMP

2.22 Produkt musi posiadać zaimplementowany moduł bezpieczeństwa (autoryzacji) w dostępie klientów danej aplikacji do wirtualnych usług serwerowych zdefiniowanych na loadbalancerze. Wymagane wsparcie dla mechanizmów Single Sign On (SSO); Multi-Domain authentication; X.509 client certificate authentication; Two Factor Authentication

2.23 Moduł autoryzacji (Pre-Authentication & SSO) musi integrować się co najmniej z bazami użytkowników zlokalizowanymi: Local Database, ActiveDirectory; Radius; RSA SecurID

2.24 Urządzenie musi oferować wsparcie dla Microsoft Remote Desktop Services (RDS)

2.25 Produkt musi zapewniać metody sprawdzania w warstwie 4 i 7 dostępności usług na serwerach produkcyjnych co najmniej poprzez następujące protokoły: ICMP, TCP, FTP, TELNET, SMTP, HTTP, HTTPS, POP3, NNTP, IMAP, DNS, RDP.

2.26 Produkt musi mieć funkcję filtracji adresów IP w oparciu o zdefiniowane listy dostępowe ACL (black list; white list) które kontrolują dostęp do zdefiniowanych na loadbalancerze wirtualnych serwisów VIP.

2.27 Produkt musi posiadać wbudowany moduł zapory Web Application Firewall WAF. Definiowanie i aktywacja reguł firewall powinna być możliwa w trybie ręcznym i automatycznym (sygnatury wykrywania i ochrony przed atakami). Zamawiający dopuszcza opcje ponoszenia czasowych dodatkowych kosztów utrzymania i auto-aktualizacji sygnatur bezpieczeństwa. W niniejszym postępowaniu jest wymagane dostarczenie serwisów utrzymania i auto-aktualizacji sygnatur bezpieczeństwa na okres 3-lat.

2.28 Produkt musi posiadać funkcjonalność Global Server Load Balancingu, która pozwala na:

- przekierowanie ruchu do najbliższego geograficznie lub lokalizacyjnie data center, poprzez odpowiednie przekierowanie zapytań DNS

- failover pomiędzy data center w przypadku niedostępności głównego ośrodka

2.29 Urządzenie musi posiadać wbudowane mechanizmy Session Persistence (trwałości sesji) co najmniej dla metod:

- Source IP (L4)
- SSL SessionID (L4)
- HTTP/HTTPS Browser-session (L7)
- HTTP/HTTPS WebClient-session (L7)
- RDP Login ID (L7)
- Port Following for mixed HTTP/HTTPS sessions
- Session reconnection for Microsoft RDS

3. Pakiet serwisowy

3.1 Produkt musi posiadać pakiet serwisowy na 1 rok producenta, z obsługą w systemie 24/7 i proaktywnym monitorowaniem oraz diagnozowaniem. Pakiet serwisowy musi uprawniać Zamawiającego do:

- dostęp do najnowszych wersji i korzystania z oprogramowania w ramach tej samej funkcjonalności udostępnione przez producenta w okresie trwania gwarancji,
- dostęp do bazy wiedzy i dokumentacji technicznej producenta,

- Next Business Day Advanced Hardware Replacement. 4. Sprzęt musi być fabrycznie nowy, pochodzić z autoryzowanego kanału dystrybucji producenta w Polsce.

Część V przedmiotu zamówienia

lp.	*nazwa licencji/ oprogramowania*
Przedłużenie wsparcia na posiadane przez Zamawiającego licencje dla systemu Archiwizacji poczty dla MS Exchange na 3 kolejne lata od dnia 11.09.2022 r.:	
a) ENTERPRISE VAULT ARCHIVE DISCOVERY 1 USER ONPREMISE STANDARD PERPETUAL LICENSE (dla 500 użytkowników); b) ENTERPRISE VAULT EMAIL MGMT 1 USER ONPREMISE STANDARD PERPETUAL LICENSE (dla 500 użytkowników); c) ENTERPRISE VAULT LEGACY EMAIL INGEST WIN 1 TB ONPREMISE STANDARD PERPETUAL LICENSE (1TB—1 licencja);	
Równoważny system archiwizacji poczty musi mieć co najmniej funkcjonalności: 1. System powinien być przeznaczony dla średnich i dużych firm, które mają rozbudowane środowiska informatyczne. Architektura oprogramowania systemu musi wspierać skalowanie wydajności poprzez dodawanie kolejnych serwerów (komponentów), które będą wykonywać zadania archiwizacyjne rozkładając obciążenie pomiędzy serwerami. 2. System musi istnieć na rynku minimum 10 lat i musi być systemem o uznanej pozycji na rynku oraz musi znajdować się w kwadracie „Leaders" lub „Visionaries" raportu Gartnera pt. „Magic Quadrant for Enterprise Information Archiving – w okresie co najmniej trzy lata wstecz. 3. System archiwizacji musi wspierać archiwizację wszystkich typów elementów, w tym elementów kalendarza dla następujących wersji systemów pocztowych Microsoft Exchange Server 2013 również z zainstalowanymi CU1-CU22, Microsoft Exchange Server 2016 również z zainstalowanymi CU1-CU12, Microsoft Exchange Server 2019 również z zainstalowanym CU1. 4. System archiwizacji musi wspierać archiwizację ruchu pocztowego wchodzącego i wychodzącego do i z Microsoft Office 365 i umożliwiać lokalne składowanie danych z możliwością pełnego przeszukiwania i zarządzania retencją. 5. System musi umożliwiać zautomatyzowaną archiwizację danych z plików PST z możliwością automatycznego wykrywania i przydzielania właściciela archiwum. Funkcjonalność wykrywania właściciela powinna wspierać integrację z Active Directory. 6. System archiwizacji musi mieć możliwość rozszerzenia funkcjonalności o archiwizację plików, danych z Microsoft SharePoint Server, przy czym zarządzanie systemem archiwizacji musi odbywać się w obrębie jednej konsoli.	

7. System archiwizacji musi mieć architekturę modułową. Oprogramowanie systemu archiwizacji musi wspierać instalację na odrębnych serwerach tworzących „farmę" systemu celem zwiększenia wydajności i przepustowości.
8. Architektura systemu musi umożliwiać rozmieszczenie konfiguracji, metadanych, indeksów oraz archiwizowanych danych na dedykowanych zasobach pamięci masowych. Dla zarchiwizowanych danych musi istnieć możliwość składowania w chmurze lub pamięci obiektowej.
9. System musi wspierać instalację bazy danych konfiguracji i metadanych na Microsoft SQL Server 2012 x64 edition (Enterprise i Standard), Microsoft SQL Server 2014 x64 edition (Enterprise i Standard), Microsoft SQL Server 2016 x64 edition (Enterprise i Standard), Microsoft SQL Server 2017 x64 edition (Enterprise i Standard)
10. Oprogramowanie systemu musi wspierać instalację na następujących systemach operacyjnych: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019.
11. Konsola administracyjna systemu musi wspierać jej uruchomienie na następujących systemach operacyjnych: Windows 8, Windows 8.1, Windows 10.
12. System musi wspierać integrację z Active Directory na poziomie funkcjonalnym Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016.
13. Uaktualnianie, upgrade, zmiana wersji – system musi zapewniać iż jakakolwiek zmiana wersji nie może powodować reorganizacji czy migracji danych w archiwach, archiwa musza być kompatybilne w górę to znaczy każda następna wersja oprogramowania musi obsługiwać archiwa utworzone z wcześniejszej wersji systemu
14. Możliwość archiwizowania tzw „social media" – zgodność z regulacją: FINRA 10-06
15. Musi istnieć mechanizm przełączania systemu w tryb backup tak by można było w sposób spójny wykonywać backup całego środowiska bez jego wyłączania z zachowaniem możliwości dostępu do zarchiwizowanych elementów (odczytywanie i odtwarzanie).

Wymagania dotyczące archiwizacji ruchu pocztowego

1. System archiwizacji musi umożliwiać archiwizację ruchu pocztowego za pośrednictwem protokołu SMTP dla dowolnego typu aplikacji. Uruchomienie archiwizacji za pośrednictwem protokołu SMTP musi odbywać się wyłącznie w oparciu o oprogramowanie systemu archiwizacji bez konieczności instalacji usługi Windows SMTP.
2. Archiwizacja SMTP musi wspierać przechwytywanie wszystkich metadanych, takich jak BCC, przynależność do listy dystrybucyjnej, informacje raportu dziennika (journal).
3. Zarchiwizowane dane zebrane za pośrednictwem protokołu SMTP muszą być dostępne dla użytkownika w osobistym archiwum z podziałem na Skrzynkę Odbiorczą i Elementy Wysłane.
4. System archiwizacji musi umożliwiać archiwizację ze skrzynek journaling-owych oprogramowania Microsoft Exchange.

5. System archiwizacji musi wspierać zarówno Standard Journaling jak i Envelope Journaling Microsoft Exchange.
6. Archiwizacja maili z skrzynek journaling-owych oprogramowania Microsoft Exchange powinna następować automatycznie, nie rzadziej niż co 5 min. Po archiwizacji wszystkie e-maile muszą być natychmiast kasowane, po to by nie dopuścić do przyrostu wielkości skrzynki journaling-owej.
7. Przypisanie retencji (czas przechowywania) musi być możliwe co najmniej na poziomie skrzynki journalingowej, a więc wszystkie maile jakie znajdą się w takiej skrzynce będą zarchiwizowane z jednakową retencją
8. System musi oferować tak zwany selektywny journaling, a więc możliwość zdefiniowania reguł filtru tego co ma być archiwizowane. System musi oferować filtrowanie na postawie: ciągu znaków adresu docelowego, nazwy listy dystrybucyjnej, nazwy domeny docelowej.

Wymagania dotyczące archiwizacji skrzynek pocztowych

1. Archiwizowanie musi odbywać się poprzez profil MS Outlook tak by nie było potrzeby instalowania oprogramowania na serwerach MS Exchange, chyba że będzie tego wymagał dostęp poprzez OWA
2. Musi umożliwiać definiowanie rożnych reguł, którym będą podlegać dane przeznaczone do archiwizacji, w szczególności dla MS Exchange musi być możliwość archiwizacji danych na podstawie kryteriów czasowych i w oparciu o procent wolnego miejsca w skrzynce (obie funkcje muszą być dostępne jednocześnie dla dowolnej skrzynki) dla tych funkcjonalności nie wymagane jest uruchamianie dodatkowych funkcjonalności na Exchange (np. journaling)
3. Po zakończeniu archiwizacji w skrzynce użytkownika muszą pozostać znaczniki maili tak by dla użytkownika końcowego dostęp do danych w archiwum był taki sam jak do danych w Exchange
4. System musi potrafić uaktualniać znaczniki tak by w razie przeniesienia ich w inne miejsce odzyskiwanie maili odbywało się bez ograniczeń.
5. Musi integrować się z funkcjonalnością „managed folders” w Microsoft Exchange.
6. Musi oferować możliwość migracji plików pst całkowicie automatycznie, także wtedy, gdy oprogramowanie MS Outlook jest wyłączone na stacjach użytkowników, po zakończeniu migracji musi być możliwość automatycznego blokowania dostępu, ukrywania czy kasowania przeniesionych plików pst
7. Musi mieć możliwość tworzenia lokalnej kopii archiwum, po to by użytkownicy mobilni mogli mieć dostęp od archiwum również gdy są nie podłączeni do sieci korporacyjnej.
8. Konfiguracja i zarządzanie migracją plików pst musi być wykonywana z tej samej konsoli co zarządzanie systemem archiwizacji.
9. Musi istnieć możliwość zdefiniowania zawartości znacznika, tak by użytkownik klienta pocztowego takiego jak Outlook Express mógł odczytać zawartość maila z archiwum, wraz z ewentualnymi załącznikami – mail jako strona WWW.

10. System musi oferować (jako opcję) możliwość definiowania reguł na bazie treści czy nagłówków wiadomości pocztowych z MS Exchange tak by można było przypisywać różne wartości dt. przechowywania tych wiadomości w archiwum, a więc różne poziomy retencji danych przechowywanych w systemie bazujące między innymi na treści czy słowach kluczowych w mailach.

Wymagania dotyczące składowania danych w archiwum

1. Rozwiązanie powinno zapewniać automatyczne kasowanie danych na podstawie czasu przetrzymywania danych tzw. retention, z tym że zdefiniowanie wielu poziomów retention nie powinno powodować zmniejszenia współczynnika deduplikacji danych w archiwum
2. Funkcjonalność deduplikacji danych musi obejmować różne typy danych tzn. plik dołączony do zarchiwizowanego maila powinien być raz zachowany w archiwum nawet wtedy gdy byłby zarchiwizowany bezpośrednio z systemów plików czy z SharePoint'a – funkcjonalność ta musi być dostępna dla dowolnych dysków i producentów sprzętu, musi być cechą oprogramowania a nie specyficznego sprzętu i być w cenie produktu
3. System powinien mieć możliwość (opcja) archiwizować dane także na taśmy, jako następny etap (poziom) składowania danych

Wymagania dotyczące zarządzania systemem archiwizacji

1. Powinno posiadać jedną centralną konsolę, która umożliwia administrowanie wszystkimi funkcjami także tymi dotyczącymi migracji plików pst, czy zarządzaniem archiwizacją zasobów plikowych czy SharePoint
2. Musi istnieć możliwość zarządzania archiwum poprzez przeglądarkę Internet Explorer
3. Musi posiadać możliwość delegowania uprawnień pomiędzy osoby (administratorów) danych komponentów np. zarządzanie storage

Wymagania dotyczące przeszukiwania archiwum

1. System archiwizacji musi tworzyć indeksy do zarchiwizowanych danych tak by można było przeszukiwać archiwa pełnokontekstowo po treści wiadomości również po treści załączników
2. System archiwizacji musi posiadać możliwość włączenia lub wyłączenia pełnokontekstowego indeksowania treści dla poszczególnych skarbców archiwum.
3. Indeksy muszą być przetrzymywane tak długo jak dane w archiwach
4. Oprogramowanie musi rozpoznawać i indeksować treść z większości popularnych i spotykanych w świecie formatów dokumentów (np. MS Office, Open Office, PDF, JPG, CAD…), ilość rozpoznawanych typów dokumentów to minimum 300
5. Reindeksowanie danych nie może blokować dostępu do archiwum dla użytkowników
6. Funkcjonalność archiwizowania maili z dziennika (journaling) z MS Exchange musi umożliwiać przeszukiwanie danych włącznie z polami BCC

7. Musi posiadać jako opcję integracje z Windows Rights Management i PGP, a więc odszyfrowywanie wiadomości pocztowych celem ich indeksacji dla celów e-Discovery
8. Musi posiadać jako opcję komponenty umożliwiające automatyczne przeszukiwanie danych na podstawie słów kluczowych, słowników, blokowanie maili przed skasowaniem, jeśli treść wskazuje na złamanie reguł lub regulacji
9. Musi posiadać oddzielna aplikację dla wykonywania zaawansowanych przeszukiwań archiwów związanych z wymaganiami działów audytu czy bezpieczeństwa, aplikacja taka musi mieć własny system autoryzacji i przedzielania uprawnień do archiwów. Aplikacja taka musi oferować zaawansowane możliwości definiowania zadań przeszukiwania danych i posiadać możliwości automatycznego cyklicznego ich uruchamiania
10. Aplikacja obsługująca zaawansowane przeszukiwania archiwów musi potrafić wykrywać zduplikowane wiadomości tak by w raportach czy przy eksportowaniu nie powielać powtarzających się maili
11. Aplikacja do przeszukiwania musi posiadać mechanizm exportu danych do formatu HTML, tak aby można było je przeglądach w przeglądarce internetowej.

Wymagania dotyczące bezpieczeństwa i nadzoru nad archiwum

1. Musi umożliwiać audytowanie wszelkich działań w systemie archiwizacyjnym w szczególności związanych ze zmianą parametrów czy kasowaniem danych z archiwum.
2. Musi umożliwiać audytowanie operacji Wyszukiwania i Wyświetlania danych z archiwum.
3. Wpis audytu musi zawierać następujące informacje: Data i godzina wystąpienia, nazwa użytego konta, nazwa użytego skarbca archiwum.
4. System archiwizacji musi udostępniać możliwość wygenerowania raportu audyt
5. System archiwizacji musi zapewniać szczegółowe raporty dotyczące aktywności archiwizacyjnych dla Microsoft Exchange. Posiadać gotowe do użycia gotowe do użycia raporty dotyczące kondycji, trendów wykorzystania, pojemności i stanu systemu archiwizacji.
6. System archiwizacji musi umożliwiać generowanie niestandardowych raportów.
7. System musi umożliwiać eksportowanie raportów do formatu PDF, HTML, XLS/XLSX, CVS, XML.
8. System archiwizacji musi posiadać dedykowany moduł dla integracji z systemem Microsoft SCOM, umożliwiający administratorom centralne śledzenie zdarzeń i aktywności.

Wymagania dotyczące dostępu do danych przechowywanych w archiwum

1. Musi posiadać możliwość dostępu do archiwum z urządzeń mobilnych, w zakresie wyszukiwania, przeglądania treści oraz pobierania danych z archiwum.
2. Musi posiadać możliwość dostępu do archiwum poprzez klienta Outlook w taki sposób że jest ono widoczne (archiwum) jako struktura folderów w Outlook'u, dzięki czemu użytkownicy mają bezpośredni dostęp do zarchiwizowanych maili bez potrzeby używania skrótów czy uruchamiania

komponentów celem operowania na archiwum, funkcjonalność musi być dostępna także wtenczas gdy Outlook pracuje w trybie offline. 3. Musi posiadać polski interfejs (plug-in) do Outlooka, dla końcowego użytkownika. 4. System archiwizacji musi posiadać dokumentację użytkownika końcowego archiwum w języku polskim.

Część VI przedmiotu zamówienia

lp.	*nazwa licencji/ oprogramowania*
Przedłużenie wsparcia na posiadane licencje na system typu SIEM na 3 kolejne lata od dnia 18.12.2022 r.:	
a) Energy Logserver Log Management Plan - Perpetual license; b) Energy Logserver SIEM Plan - Perpetual license.	
Równoważny system musi mieć co najmniej funkcjonalności: 1. System musi wykorzystywać nierelacyjną, rozproszoną bazę danych opartą o Elasticsearch w wersji minimum 7.x 2. System musi pracować w oparciu o architekturę Linux. 3. System musi mieć możliwość centralnego zbierania i zarządzania logami 4. System musi działać w trybie zbliżonym do rzeczywistego 5. System musi zapewniać efektywną obsługę co najmniej 500 PS lub 40GB danych dziennie 6. System musi zapewniać retencję danych w okresie minimum 60 dni. 7. System musi zapewniać możliwość jednoczesnej pracy dla co najmniej 10 jednoczesnych użytkowników. 8. System nie może limitować ilości jednocześnie pracujących użytkowników. 9. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska. 10. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja. 11. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu. 12. System musi mieć możliwość zapewnienia wysokiej dostępność na poziomie Agregacji i Retencji (na tym etapie postępowania nie jest to wymagane) 13. System musi mieć możliwość buforowania agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie po przywróceniu pełnej sprawności systemu (na tym etapie postępowania nie jest to wymagane) .	

14. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.
15. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protoków TLS w wersji minimum 1.3.
16. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
17. Interfejs musi posiadać angielską lub polską wersję językową.
18. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). System powinien spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).

Dostęp do systemu

19. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
20. Autoryzacja do systemu musi być zintegrowana z:
    - Microsoft AD
    - LDAP
    - Radius
21. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
22. System musi wspierać mechanizm logowania typu Single Sign On.
23. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
24. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
25. System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only" oraz „pełny". Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
26. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
27. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
28. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
29. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.

Przyjmowanie, identyfikacja i wizualizacja danych

30. System musi pozwalać na tworzenie parserów z poziomu GUI

31. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
32. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
33. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
34. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
35. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
36. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:
    - Syslog,
    - WEF,
    - Flat file,
    - Event log,
    - WMI,
    - SNMP trap,
    - XML,
    - JSON,
    - CSV,
    - Email,

    Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.
37. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
38. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
39. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
40. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
41. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.

42. System musi posiadać predefiniowany zestaw parserów zdarzeń.
43. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
44. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie
45. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
46. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
47. System musi umożliwiać integrację z Mitre ATT@CK
48. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
49. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
50. Proces parsowania musi umożliwiać wzbogacanie treści odbieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
51. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzne procedury bezpieczeństwa.
52. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
53. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.

Systemy źródłowe z których system musi zbierać logi min.:

- Microsoft Windows Server
- Linux
- Bind
- Apache
- IIS
- SQL
- MYSQL
- Firewall (PaloAlto, Checkpoint, Fortigate)
- Lotus Domino
- Microsoft Exchange
- Microsoft NPS
- File Server

- Load Balancer (F5, KEMP)
- Hyper-v
- VMware (vSphare)
- Switche (Cisco, Aruba, DELL)
- WiFi (Cisco, Aruba)
- Bramka Pocztowa (Barracuda, Symantec, Trend Micro)
- Serwery Rac (Dell, HP, Fujitsu)
- NextCloud
- System Antywirusowy (Eset)

Reguły korelacyjne, alerty i obsługa incydentów:

54. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
55. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
56. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych.
57. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
58. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
    - Wykrycia dowolnej treści w logach,
    - Wykrycia wystąpienia wartości pola na wybranej liście,
    - Wykrycia niewystępowania wartości pola na wybranej liście,
    - Wykrycia zmiany jednego z kilku pól,
    - Wykrycia zdarzeń występujących z zadaną częstotliwością,
    - Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
    - Wykrycia zaniku Wiadomości,
    - Wykrycia nowej wartości pola w zadanym okresie czasu,
    - Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
59. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów.
60. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
61. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
62. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych.

63. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności.
64. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
65. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
66. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
67. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
68. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
69. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
70. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
71. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
72. System musi dostarczać funkcjonalność badania integralności plików i rejestrów na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
73. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
74. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST oraz CIS
75. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
76. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows.
77. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP.
78. System musi umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule.
79. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.

Raportowanie i Archiwizacja danych:

80. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
81. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
82. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
83. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
84. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
85. Mechanizm archiwizacji musi umożliwiać na przywracanie danych do systemu celem analiz online.
86. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.

Załącznik nr 2 do zapytania o wycenę

FORMULARZ WYCENY

Wykonawca (pełna nazwa albo imię i nazwisko)		
siedziba/miejsce zamieszkania i adres, jeżeli jest miejscem wykonywania działalności Wykonawcy		
w zależności od podmiotu numer KRS		
imię nazwisko, stanowisko/podstawa do reprezentacji		
NIP/REGON		
telefon		
e-mail		
osoba do kontaktów z Zamawiającym		
Czy Wykonawca jest mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem[1]?	[ ] Tak	[ ] Nie

Ministerstwo Edukacji i Nauki
ul. Wspólna 1/3
00-529 Warszawa

W odpowiedzi na zapytanie o wycenę oprogramowania dla Ministerstwa Edukacji i Nauki (sprawa: BDG-WII.262.14.2022), przedstawiam wycenę sporządzoną w oparciu o opis Zamawiającego, jak niżej:

[1] Por. ***zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36). Te informacje są wymagane wyłącznie do celów statystycznych. Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR. Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR. Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami*** i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR *lub* roczna suma bilansowa nie przekracza 43 milionów EUR.

Część I

Przedłużenie wsparcia na posiadane przez Zamawiającego licencje wraz ze sprzętem na system Antyspamowy Symantec Messaging Gateway na 3 kolejne lata od dnia 02.11.2022 r.

Lp.	Nazwa	Ilość	Cena brutto za 1 szt. PLN	Wartość brutto PLN
1	*2*	*3*	*4*	*5*
1	End Customer SMG Support, Next Business Day Delivery Hardware Support – wsparcie dla appliance	2	……	…….
2	Messaging Gateway Initial Subscription License with Support ACD-GIV 500-999 User 3TR	800	……	…….
			RAZEM	…….
słownie złotych: ……..……..……				

Część II

Lp.	Nazwa	Ilość	Cena brutto za 1 szt. PLN	Wartość brutto PLN
1	*2*	*3*	*4*	*5*
1	Zakup wieczystej licencji typu Academic dla MS Exchange 2019 Standard z możliwością upgrade do nowszej wersji przez okres 3 lat	3	……	…….
2	Zakup wieczystej licencji typu Academic dla MS Exchange Server Standard 2019 User CAL z możliwością upgrade do nowszej wersji przez okres 3 lat	500	……	…….
3	Zakup wieczystej licencji typu Academic dla Microsoft Office Standard 2021	500	……	…….
4	Zakup wieczystej licencji typu Academic dla MS Windows Server Datacenter 2022 per core	176	……	…….
5	Zakup wieczystej licencji typu Academic dla MS Windows Server user CAL per core	500	……	…….
6	Zakup wieczystej licencji typu Academic dla MS Windows Server Standard 2022 per core	56	……	…….
7	Zakup wieczystej licencji typu Academic dla Windows Server 2022 RDS User CAL	140	……	…….
9	Migracja MS Exchange 2016 do MS Exchange 2019			…….
10	Szkolenia dla zaoferowanych Systemów			…….
			RAZEM	…….
słownie złotych: ……..……..……				

Część III

Lp.	Nazwa	Ilość	Cena brutto za 1 szt. PLN	Wartość brutto PLN
1	*2*	*3*	*4*	*5*
1	Przedłużenie posiadanych licencji ADSelf Service Professional na 3 kolejne lata od dnia 07.12.2022 r.	500	…….	…….
			RAZEM	…….
słownie złotych: ……				

Część IV

Przedłużenie wsparcia na posiadane przez Zamawiającego licencje wraz ze sprzętem na system Kemp Loadbalancer na 3 kolejne lata od dnia 10.09.2022 r.

Lp.	Nazwa	Ilość	Cena brutto za 1 szt. PLN	Wartość brutto PLN
1	*2*	*3*	*4*	*5*
1	ENP-LM-X3 – 3 Year Enterprise Plus Subscription for LoadMaster LM-X3. Includes 7x24 Telephone & E-Mail Support Next Business Day Advanced Replacement Hardware Maintenance security notifications hotfixes software updates KEMP 360 Central management and automation KEMP	2	……	…….
			RAZEM	…….
słownie złotych: ……				

Część V

Przedłużenie wsparcia na posiadane przez Zamawiającego licencje dla systemu Archiwizacji poczty dla MS Exchange na 3 kolejne lata od dnia 11.09.2022 r.

Lp.	Nazwa	Ilość	Cena brutto za 1 szt. PLN	Wartość brutto PLN
1	*2*	*3*	*4*	*5*
1	Przedłużenie wsparcia dla ENTERPRISE VAULT ARCHIVE DISCOVERY 1 USER ONPREMISE STANDARD PERPETUAL LICENSE	500	……	…….
2	Przedłużenie wsparcia dla ENTERPRISE VAULT EMAIL MGMT 1 USER ONPREMISE STANDARD PERPETUAL LICENSE	500	……	…….
3	Przedłużenie wsparcia dla ENTERPRISE VAULT LEGACY EMAIL INGEST WIN 1 TB ONPREMISE STANDARD PERPETUAL LICENSE	1	……	…….
			RAZEM	…….
słownie złotych: ……				

Część VI

Przedłużenie wsparcia na posiadane licencje na system typu SIEM na 3 kolejne lata od dnia 18.12.2022 r.

Lp.	Nazwa	Ilość	Cena brutto za 1 szt. PLN	Wartość brutto PLN
1	*2*	*3*	*4*	*5*
1	Przedłużenie wsparcia dla Energy Logserver Log Management Plan - Perpetual license	1	……	…….
2	Przedłużenie wsparcia dla Energy Logserver SIEM Plan - Perpetual license	1	……	…….
			RAZEM	…….
słownie złotych: ……				

podpis osoby/osób uprawnionej/uprawnionych do reprezentowania Wykonawcy(pieczątki)

…… (miejscowość) , dnia …… (data) r.