Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Numer sprawy: RIOŚ.Z.271.15.2023 Opinogóra Górna, dnia 14 lipca 2023 r.

Szczegółowy Opis Przedmiotu Zamówienia

na dostawę sprzętu i oprogramowania związaną z realizacją projektu
w ramach grantu „Cyfrowa Gmina”

Spis treści

1. Zestawienie ilościowe.

Lp.	Nazwa	Ilość
1.	Doposażenie serwerowni - zakup serwera wraz z oprogramowaniem	1
2.	Doposażenie serwerowni - zakup urządzenia NAS	1
3.	Doposażenie serwerowni - zakup dysków do istniejącego serwera	6
4.	Doposażenie serwerowni - zakup UPS	1
5.	Doposażenie serwerowni - zakup oprogramowania backup	1
6.	Doposażenie serwerowni - zakup oprogramowania do wirtualizacji	1
7.	Doposażenie serwerowni - zakup urządzenia UTM	1
8.	Zakup usług wdrożenia i konfiguracji środowiska IT	1

2. Przedmiot zamówienia.

2.1. Wymagania ogólne w zakresie dostawy sprzętu.

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowany nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.

11. Dla dostaw sprzętu informatycznego z systemem operacyjnym Zamawiający wymaga fabrycznie nowego systemu operacyjnego (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego systemu operacyjnego nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku systemu operacyjnego naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

2.2. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.

7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić na komputerze o oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić na komputerze o oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego

w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

2.3. Doposażenie serwerowni - zakup serwera wraz z oprogramowaniem (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa RACK o wysokości maksymalnie 1U z możliwością instalacji min. 8 dysków 2.5 cala wraz z kompletem wysuwanych szyn wraz z organizerem okablowania umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych.
2. Zainstalowany jeden procesor dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 256 punktów w teście SPECrate®2017_fp_base organizacji Standard Performance Evaluation Corporation (www.spec.org) określonego dla konfiguracji dwuprocesorowej. Zamawiający żąda przedłożenia testu potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności na etapie procedury odbiorowej.
3. Pamięć RAM: min. 256 GB, minimum 10 wolnych slotów pamięci.
4. Zabezpieczenia pamięci RAM (minimum dwa z wymienionych): Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub RAM Advanced ECC i/lub Memory Page Retire i/lub Fault Resilient Memory i/lub Memory Self-Healing.
5. Gniazda PCI: min. dwa aktywne sloty PCIe min. Gen 4.
6. Interfejsy sieciowe: minimum 4 porty typu Gigabit Ethernet Base-T oraz minimum 2 porty typu 10GbE SFP+.
7. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD.
8. Zainstalowane 6 dysków twardych SAS o pojemności: 2 x min. 600 GB SAS każdy oraz 4 x min. 1,2 TB SAS każdy. Dyski w konstrukcji Hot Plug z prędkością min. 12 Gb/s każdy. W przypadku

uszkodzenia dysków w okresie gwarancji Zamawiający wymaga by uszkodzone dyski pozostały jego własnością.

9. Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający min. 4 GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0/1/5/6/10/50/60.
10. Wbudowane porty: min. 3 porty USB, 1 port VGA.
11. Dodatkowe karty: zintegrowana karta graficzna.
12. Wbudowany moduł TPM 2.0.
13. Zasilanie: Zasilacze redundantne typu Hot Plug.
14. Chłodzenie: Wentylatory zapewniające odpowiednią pracę urządzenia.
15. Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    a. zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
    b. zdalne monitorowanie i informowanie o statusie serwera w zakresie minimum temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe,
    c. szyfrowane połączenie oraz autentykacje i autoryzację użytkownika,
    d. wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
    e. wirtualną konsolę z dostępem do myszy, klawiatury,
    f. wsparcie dla IPv6,
    g. wsparcie dla SNMP, IPMI2.0, VLAN tagging, SSH,
    h. integracja z Active Directory.
16. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
17. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda przedłożenia dokumentów potwierdzających spełnienie przez oferowany serwer i jego producenta w zakresie określonym powyżej na etapie procedury odbiorowej.
18. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard 2022 lub równoważnego zgodnie z poniżej określonymi warunkami równoważności wraz z licencjami umożliwiającymi jednoczesny dostęp do zasobów oprogramowania zarządzającego serwerem dla 30 użytkowników.

Warunki równoważności dla dostawy oprogramowania klasy Microsoft Windows Serwer Standard 2022:

a. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
b. Możliwość wykorzystania, co najmniej 120 logicznych procesorów oraz co najmniej 2 TB pamięci RAM w środowisku fizycznym.
c. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
d. 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.
e. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
f. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
g. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
h. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
i. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
j. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
k. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
l. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
m. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
n. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
o. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
p. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
q. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
r. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
s. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
t. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
u. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

v. O ile to konieczne ze względu na licencjonowanie producenta oferowanego serwerowego systemu operacyjnego Zamawiający wymaga dostarczenia licencji dostępowych dla 30 użytkowników.

19. Gwarancja: min. 36 miesięcy gwarancji producenta z czasem reakcji w miejscu instalacji sprzętu w następny dzień roboczy. Możliwość rozszerzenia pakietu gwarancyjnego na serwis z gwarantowanym czasem naprawy w ciągu 6 godz. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. W okresie gwarancji wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Serwis musi zawierać usługę pozostawiania u Zamawiającego uszkodzonych dysków w okresie obowiązywania gwarancji bez dodatkowych opłat.

Dodatkowo, w ramach oprogramowania Zamawiający oczekuje dostawy oprogramowania do zarządzania siecią i zasobami IT o poniżej określonych parametrach minimalnych:

1. Oprogramowanie musi składać się serwera zarządzającego, zdalnych konsoli oraz Agentów.
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2.
3. Oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.
4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów - nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników.
5. Oprogramowanie musi posiadać funkcjonalność monitorowania infrastruktury serwerowej i sieciowej w zakresie:
   a. wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
   b. wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
   c. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
   d. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
   e. serwerów pocztowych: - monitorowanie serwisu odbierającego, jak i wysyłającego pocztę, - możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), - możliwość wykonywania operacji testowych, - możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa,
   f. monitorowania serwerów WWW i adresów URL,
   g. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
   h. obsługi komunikatów syslog i pułapek SNMP.
   i. monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych- ruchu generowanego przez podłączone stacje robocze,
   j. kontroli nad monitorem usług Windows,
   k. monitorowania wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

6. Oprogramowanie musi umożliwiać automatyczne gromadzenie danych o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie:
   a. informacji dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.;
   b. zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;
   c. informacji o zainstalowanych aplikacjach oraz aktualizacjach Windows, umożliwiających audytowanie i weryfikację użytkowania licencji w organizacji;
   d. informacji o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.;
   e. możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera;
   f. możliwość odczytania numeru seryjnego (klucze licencyjne);
   g. możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;
   h. możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
7. Oprogramowanie musi mieć możliwość prowadzenia bazy ewidencji majątku IT w zakresie:
   a. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
   b. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz, możliwość importu danych z zewnętrznego źródła np. (.CSV);
   c. generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania;
   d. archiwizacji i porównywania audytów środków trwałych;
   e. tworzenia kodów kreskowych w Środkach Trwałych;
   f. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy;
   g. inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej co najmniej na system Android;
   h. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji dodatkowego oprogramowania poprzez manualne wykonanie skanów inwentaryzacji offline).
8. Oprogramowanie musi zapewniać funkcjonalność w zakresie monitorowania aktywności użytkowników na stacjach roboczych w zakresie:
   a. faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy);

b. monitorowania procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika);
c. użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona);
d. informacji o edytowanych przez użytkownika dokumentach;
e. historii pracy (cykliczne zrzuty ekranowe);
f. listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
g. transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
h. wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek.

9. Oprogramowanie musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
   a. skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie, archiwów ZIP;
   b. zarządzanie posiadanymi licencjami;
   c. audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji;
   d. zarządzanie posiadanymi licencjami: raport zgodności licencji;
   e. możliwość przypisania do programów numerów seryjnych, wartości itp.
10. Oprogramowanie musi zapewniać integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
11. W zakresie pomocy technicznej system musi umożliwiać:
    a. tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów);
    b. załączanie komentarzy, zrzutów ekranów i załączników w zgłoszeniach;
    c. konfigurowanie pól niestandardowych, powiązanych w wybraną kategorią zgłoszenia;
    d. przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach”);
    e. dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę;
    f. planowanie zastępstw w przydzielaniu zgłoszeń;
    g. funkcję rozbudowanych raportów;
    h. powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym;
    i. baza zgłoszeń z rozbudowaną wyszukiwarką;
    j. przejrzysty i intuicyjny interfejs webowy;
    k. wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych;
    l. komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu;
    m. zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury;
    n. dwukierunkowa wymiana plików;
    o. zarządzanie procesami Windows z poziomu okna informacji o urządzeniu;

p. zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania);
q. procesowanie zgłoszeń z wiadomości e-mail;
r. integracja bazy użytkowników z Active Directory;
s. zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).

12. W zakresie kontroli dostępu do danych system musi umożliwiać:
    a. automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa;
    b. ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych;
    c. zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych;
    d. integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania;
    e. integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych;
    f. możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB);
    g. alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”);
    h. integracja z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów
    i. zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami;
    j. informacje o urządzeniach podłączonych do danego komputera;
    k. lista wszystkich urządzeń podłączonych do komputerów w sieci;
    l. audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych;
    m. zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników;
    n. centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory.

<u>Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:</u>

1. Instalacja ma odbyć się na wszystkich komputerach oraz serwerach posiadanych przez Zamawiającego – 30 użytkowników.
2. Zamawiający dopuszcza instalację i wdrożenie zdalne.
3. Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
4. Wykonawca będzie udzielał pomocy technicznej Zamawiającemu przez okres gwarancji.
5. Usługa wsparcia wdrożenia obejmuje:
    a. analizę przedwdrożeniowa,
    b. pomoc przy instalacji silnika bazy danych - jeżeli będzie wymagana instalacja,
    c. instalację oprogramowania: na stacji roboczej,
    d. dystrybucję oprogramowania na wybranych stacjach roboczych,
    e. konfigurację oprogramowania,
    f. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
    g. szkolenie administratorów z zakresu pracy z programem:

h. przykładowy audyt oprogramowania i plików na wybranej stacji roboczej,
i. generowanie raportów i zestawień dotyczących sprzętu, oprogramowania i użytkowników,
j. użytkowanie zdalnego pulpitu.
k. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połącznie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.

Wymagania licencyjne dla dostarczonego oprogramowania:

1. Licencjobiorcą wszystkich licencji będzie Gmina Opinogóra Górna.
2. Licencje muszą zostać wystawione na czas nieoznaczony (bezterminowy).
3. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
4. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do rozbudowy, zwiększenia ilości serwerów obsługujących oprogramowanie, przeniesienia oprogramowania na inny serwer, rozdzielenia funkcji serwera (osobny serwer bazy danych, osobny serwer aplikacji, osobny serwer plików).
5. Licencja oprogramowania musi być licencją bez ograniczenia ilości komputerów, serwerów, na których można zainstalować i używać oprogramowanie.
6. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
7. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
8. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
9. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).
10. Wykonawca zapewni minimum 24 miesięczną gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.

2.4. Doposażenie serwerowni - zakup urządzenia NAS (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa do szafy RACK.
2. Procesor wielordzeniowy osiągający w teście wydajności PassMark Performance Test co najmniej wynik 20 000 punktów, testy powinny być aktualne w okresie nie dłuższym niż 30 dni przed składaniem ofert. Zamawiający żąda raportu z oprogramowania testującego potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności na etapie procedury odbiorowej.
3. Pamięć RAM: min. 32 GB.
4. Pamięć flash: min. 4 GB.

5. Funkcje: wsparcie dla wirtualizacji, scentralizowana pamięć masowa na dane, backup, udostępnianie i przywracanie systemu po awarii.
6. Możliwość zainstalowania łącznie 12 dysków, min. SATA 3 - 6 Gb/s.
7. Zainstalowane dyski: min. 12 x dysk SSD 2,5" SATA 2 TB.
8. Poziom RAID: 1,5,6.
9. Kompatybilność dysków: 3,5-calowe dyski twarde SATA; 2,5-calowe dyski twarde SATA; 2,5-calowe dyski SSD SATA.
10. Obsługa połączeń 10GbE SFP+ (co najmniej dwa porty) oraz 10 GbE RJ45 (co najmniej dwa porty) wraz z 2 wkładkami 10GbE SFP+ do NAS oraz niezbędnymi kablami do połączenia NAS z przełącznikiem za pomocą wszystkich interfejsów w tym dwie wkładki 10GbE SFP+ do podłączenia do posiadanego przez Zamawiającego przełącznika. Dodatkowo GbE RJ45 (co najmniej dwa porty)
11. Porty USB: min. 4x USB 3.0.
12. Szyny do montażu w szafie RACK.
13. Gwarancja producenta min. 36 miesięcy realizowanej w miejscu instalacji sprzętu, z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia. Gwarancja musi obejmować także dyski. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.

2.5. Doposażenie serwerowni - zakup dysków do istniejącego serwera (6 szt.).

Zadanie przewiduje dostawę sześciu dysków do istniejącego serwera ..... o numerze seryjnym .....

Dyski powinny być wykonane w technologii Hot Plug o pojemności nie mniejszej niż 1.2TB HDD SAS każdy o prędkości min. 12Gb/s, 10 k obr/min. Dyski powinny zostać objęte gwarancją producenta na minimum 36 miesięcy i być kompatybilne z serwerem.

2.6. Doposażenie serwerowni - zakup UPS (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: RACK o rozmiarze maksymalnym 3U.
2. Moc pozorna: minimum 3000 VA.
3. Moc rzeczywista: minimum 2700 Wat.
4. Architektura UPSa: line-interactive lub on-line
5. Liczba i rodzaj gniazdek z utrzymaniem zasilania: min. 6 szt. C13/C19.
6. Czas podtrzymania dla obciążenia 100%: min. 3 min.
7. Czas podtrzymania przy obciążeniu 50%: min. 11 min.
8. Interfejsy: 1 x USB, 1 x RJ45.
9. Funkcje: zimny start, awaryjne wyłączanie zasilania, ochrona przed nagłym wzrostem napięcia, baterie wymienne podczas pracy urządzenia, automatyczny test baterii.
10. Wyświetlacz LCD.
11. Gwarancja producenta min. 24 miesiące (w tym na baterię).

2.7. Doposażenie serwerowni - zakup oprogramowania backup (1 szt.).

Minimalne parametry:

1. Wymagania ogólne:
   - licencja wieczysta na oprogramowanie ma umożliwiać backup 10 (z możliwością rozszerzenia do 50) dowolnych środowisk;
   - oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019;
   - oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami;
   - oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V;
   - oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
2. Całkowite koszty posiadania:
   - oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej;
   - oprogramowanie musi tworzyć „samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków;
   - oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy;
   - oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów;
   - oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli;
   - oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu;
   - oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota;
   - oprogramowanie musi oferować portal umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time);
   - oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API;
   - oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji;
   - oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej;

- oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji konsol administracyjnych.

3. Wymagania RPO:
   - oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji;
   - oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych;
   - oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn;
   - oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN;
4. Wymagania RTO:
   - oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych;
   - dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna);
   - oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny;
   - oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre;
   - oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków;
   - oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny;
   - oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej;
   - oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
5. Monitoring:
   - system musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich;
   - system musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn;

- system musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej;
- system musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora;
- system musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej;
- system musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego;
- system musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

6. Raportowanie:
   - system raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej;
   - system musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc;
   - system musi mieć możliwość ustawienia harmonogramu generowania raportów;
   - system musi mieć możliwość generowania raportów z dowolnego punktu w czasie;
   - system musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.

2.8. Doposażenie serwerowni - zakup oprogramowania do wirtualizacji (1 szt.).

Minimalne parametry funkcjonalne oprogramowania:

1. Warstwa wirtualizacji oprogramowania powinna umożliwiać instalację bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić wymóg obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagany jest wymóg przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
3. Oprogramowanie do wirtualizacji musi zapewnić wymóg skonfigurowania maszyn wirtualnych z możliwością dostępu do min. 4TB pamięci operacyjnej.
4. Oprogramowanie do wirtualizacji musi zapewnić wymóg przydzielenia maszynom wirtualnym do 64 procesorów wirtualnych.
5. Licencja dostarczonego oprogramowania powinna umożliwiać działanie na minimum trzech serwerach fizycznych.
6. Oprogramowanie do wirtualizacji zapewniać powinno możliwość skonfigurowania maszyn wirtualnych.
7. Oprogramowanie do wirtualizacji zapewniać powinno możliwość stworzenia dysku maszyny wirtualnej.

8. Rozwiązanie powinno umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
9. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
10. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna ma mieć możliwość działania na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna.
11. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH. z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
12. Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej.
13. Oprogramowanie do wirtualizacji powinno zapewniać możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
14. Rozwiązanie powinno zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
15. Oprogramowanie do wirtualizacji musi zapewnić wymóg klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
16. Rozwiązanie powinno mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
17. Wykonawca powinien zapewnić możliwość funkcjonowania oprogramowania zgodnie z określonymi wymaganiami w okresie minimum 24 miesięcy. W okresie udzielonej gwarancji Wykonawca jest zobowiązany zapewnić wsparcie producenta oferowanego oprogramowania umożliwiające co najmniej aktualizację oprogramowania do najnowszych wersji.

2.9. Doposażenie serwerowni - zakup urządzenia UTM (1 szt.).

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.

System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.

2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

Minimalne parametry techniczne urządzenia:

1. Przepustowość Firewall: min. 10 Gbps.
2. Musi obsługiwać min. 700 000 jednoczesnych połączeń.
3. Musi obsługiwać co najmniej 200 połączeń VPN.
4. Wydajność IPsec VPN: min. 6,5 Gbps.
5. Wydajność SSL VPN: min. 900 Mbps.
6. Automatyczna aktualizacja plików sygnatur antywirusowych.
7. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
8. Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.
9. Automatyczna aktualizacja sygnatur IPS.
10. IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.
11. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
12. Ilość interfejsów sieciowych: minimum 5 portów Gigabit Ethernet RJ-45. Interfejsy te powinny być skonfigurowane jako jeden z trzech rodzajów wymaganych stref bezpieczeństwa.
13. Wsparcie VLAN: Musi posiadać minimum 50 sieci VLAN.
14. Administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania.
15. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
    a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
    b. Kontrola Aplikacji.
    c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
    d. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
    e. Ochrona przed atakami - Intrusion Prevention System.
    f. Kontrola stron WWW.
    g. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
    h. Zarządzanie pasmem (QoS, Traffic shaping).
    i. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
    j. Analiza ruchu szyfrowanego protokołem SSL.
    k. Analiza ruchu szyfrowanego protokołem SSH.
16. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
17. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

18. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
19. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
20. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
21. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
22. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
23. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
24. 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.
25. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
26. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
27. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
28. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
29. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
30. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
31. Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
32. Urządzenie powinno mieć możliwość generowania raportów.
33. 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.
34. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
35. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
36. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
37. 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.
38. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
39. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować

następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres gwarancji urządzenia.

40. Gwarancja producenta min. 36 miesięcy. Gwarancja powinna obejmować również możliwość wymiany urządzenia na nowe w przypadku wady urządzenia UTM.

2.10. Zakup usług wdrożenia i konfiguracji środowiska IT (1 szt.).

1. Wykonawca ma obowiązek zainstalować wszystkie urządzenia w szafie RACK oraz dokonać ich uruchomienia zgodnie z wytycznymi Zamawiającego. Wykonawca zainstaluje w serwerze dostarczane dyski. Czynności te będą wykonywane w porozumieniu z Zamawiającym oraz pod nadzorem Zamawiającego. Wykonawca wykonana aktualizację oprogramowania i firmware'ów na urządzeniach, musi zostać wykonana konfiguracja sieci do pracy urządzeń w środowisku Zamawiającego, musi zostać wykonana konfiguracja i udostępnienie zasobów. Muszą zostać wykonane testy akceptacyjne polegające na weryfikacji poprawności pracy serwera oraz zainstalowanych na nim usług i ich komunikacji z innymi urządzeniami. Musi zostać przygotowana dokumentacja powykonawcza zainstalowanych urządzeń oraz wykonanych prac instalacyjno-konfiguracyjnych.
2. Wykonawca wykona wszystkie połączenia logiczne SAN i LAN oraz dokona konfiguracji dostarczonych urządzeń zgodnie z zaleceniami Zamawiającego.
3. Rozprowadzi okablowanie logiczne LAN i SAN oraz kable energetyczne w serwerowni wewnątrz szafy RACK.
4. Wykonawca czytelnie (przy użyciu drukarki etykiet) oznaczy rozprowadzone okablowanie zgodnie z przyjętą nomenklaturą nazewnictwa przekazana przez Zamawiającego.
5. Wykonawca przeprowadzi instalację i konfigurację wszystkich elementów oprogramowania do wirtualizacji wymaganych przez Zamawiającego na dostarczanym serwerze. Wykonawca przygotuje maszyny wirtualne dla istniejącego oprogramowania w ilości minimum 12. Zamawiający odpowiada za przeniesienie/migrację istniejącego oprogramowania na maszyny wirtualne.
6. Wykonawca uruchomi i skonfiguruje oprogramowanie do wirtualizacji tak, aby było w pełni funkcjonalne we wszystkich czterech aspektach: serwerowym, dyskowym, sieciowym i zarządzania.
7. Wykonawca skonfiguruje urządzenie UTM w zakresie obejmującym minimum: aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta; aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email etc.); konfiguracja routingów statycznych na firewallu, konfiguracja polityki bezpieczeństwa (reguły dostępu dla ruchu z Internetu, do Internetu oraz między pozostałymi strefami) zgodnie z wytycznymi ze strony Zamawiającego; konfiguracja filtracji stron WWW na podstawie kategorii oraz treści; integracja UTM z systemem autoryzacji Microsoft Active Directory tak aby możliwa była identyfikacja użytkowników; konfiguracja dostępu zdalnego SSL VPN (VPN Client, portal WebVPN) dla 20 użytkowników; konfiguracja SSL descryption łącznie z instalacją certyfikatów na stacjach klienckich np. przy użyciu funkcjonalności AD, migracja istniejących polityk bezpieczeństwa funkcjonujących na istniejącym urządzeniu UTM.
8. Zamawiający wymaga kompleksowego uruchomienia i zainstalowania dostarczonego sprzętu oraz oprogramowania, w tym m. in.: konfiguracja i instalacja serwera, urządzenia NAS, dysków, oprogramowania backup, oprogramowania do wirtualizacji, podłączenie wszystkich urządzeń do

infrastruktury sieciowej zgodnie z wytycznymi Zamawiającego, instalacja serwerowego systemu operacyjnego, uruchomienie wirtualizacji zgodnie z wymaganiami Zamawiającego; instalacja i konfiguracja wirtualnych instancji serwerowego systemu operacyjnego; konfiguracja backup oraz maszyn wirtualnych na urządzeniu NAS; opracowanie, instalacja i konfiguracja systemu do wirtualizacji serwera mającego na celu podniesienie wydajności środowiska przy zachowaniu najwyższego poziomu dostępności usług zainstalowanych w tym środowisku; wdrożenie spójnych polityk zabezpieczeń mających na celu podniesienie poziomu bezpieczeństwa systemu.

9. Wykonawca przeprowadzi instalację i konfigurację oprogramowania do wykonywania backupu i odzyskiwania danych środowiska z wykorzystaniem urządzenia NAS z uwzględnieniem oprogramowania wirtualizacyjnego i serwerów.
10. Wykonawca skonfiguruje repozytoria kopii zapasowych na zasobach utworzonych na urządzeniu NAS i skonfiguruje zadania wykonywania kopii zapasowych zgodnie z wymaganiami Zamawiającego.
11. Wykonawca dokona migracji kontrolera domeny i postawienie zapasowego kontrolera (na maszynę wirtualną).
12. Wykonawca dokona migracji folderów sieciowych z uprawnieniami na maszynę wirtualną.
13. Proces współpracy w zakresie prac instalacyjno-konfiguracyjnych:
    a. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne i instalacyjne, po wykonaniu analizy istniejących u Zamawiającego rozwiązań wraz z koncepcją wdrożenia infrastruktury programowo-sprzętowej uwzględniając obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
        i. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych (jeśli są wymagane), uwzględniający specyfikę organizacji Zamawiającego,
        ii. opis koncepcji realizacji prac,
        iii. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
    b. Akceptacja projektu technicznego wraz z procedurami będzie podlegała następującej procedurze:
        i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami, w terminie nie dłuższym niż 10 dni kalendarzowych od dnia zawarcia umowy,
        ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
        iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
        iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
        v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,

vi. zatwierdzony projekt techniczny wraz z procedurami zostanie przekazany Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.

c. Wykonawca zrealizuje zamówienie zgodnie z zakresem prac i projektem technicznym.

d. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.

14. Zamawiający przewiduje przeprowadzenie instruktaży dla administratora rozwiązania zgodnie z poniżej określonymi wymaganiami:

a. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.

b. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.

c. Instruktaże powinny trwać minimum 16 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób.

d. Administrator rozwiązania po zakończeniu Instruktaży stanowiskowych musi w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinien znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinien umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.