Zadanie realizowane w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020
Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU
działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00

Załącznik nr 6 do SWZ

Szczegółowy opis przedmiotu zamówienia

Nazwa zamówienia:

Dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina",

Zamawiający:

Gmina Czarny Dunajec
ul. Józefa Piłsudskiego 2, 34-470 Czarny Dunajec

Znak sprawy**:** **RB.271.17.2022**

Kwiecień 2022

Spis treści

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

- całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
- całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

2. Wymagania gwarancyjne.

Sprzęt

- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
- Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
- Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;
- wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

Oprogramowanie

- oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

3. Ubezpieczenie sprzętu

Wykonawca zobowiązany jest do dostawy sprzętu komputerowego wraz z ubezpieczeniem na okres 12 m-cy. Koszty ubezpieczenia należy ująć w cenie oferowanego sprzętu.
Sprzęt musi zostać ubezpieczony do 100% jego wartości księgowej brutto.
Ubezpieczenie nie może przewidywać franszyzy, integralnej i udziału własnego ze strony Zamawiającego.
Polisa ubezpieczeniowa powinna zostać wystawiona na rzecz Zamawiającego.
Dostarczony sprzęt powinien zostać objęty ubezpieczeniem od wszelkich ryzyk zgodnie z poniższymi założeniami:

1. Przedmiotem ubezpieczenia jest sprzęt elektroniczny stacjonarny zainstalowany na stałe w miejscu ubezpieczenia oraz sprzęt przenośny, pod warunkiem, że wiek sprzętu elektronicznego stacjonarnego i sprzętu przenośnego nie przekracza 5 lat.
2. Sprzęt przenośny używany poza lokalem na terenie Rzeczypospolitej Polskiej jest objęty ochroną w przypadku jego utraty wskutek kradzieży z włamaniem, jeżeli został skradziony z samochodu, gdy:
    a. pojazd posiadał twardy dach (jednolitą sztywną konstrukcję),
    b. został prawidłowo zamknięty na wszystkie możliwe zabezpieczenia znajdujące się w pojeździe,
    c. był zaparkowany w zamkniętym garażu lub na parkingu strzeżonym (jeżeli kradzież z włamaniem nastąpiła w godzinach 22.00 - 6.00),
    d. ubezpieczony przedmiot był przechowywany wewnątrz pojazdu w sposób uniemożliwiający zobaczenie go z zewnątrz, np. w bagażniku.
3. Zakres ubezpieczenia:
    1) Od wszystkich ryzyk z rozszerzeniem o użytkowanie mobilne w tym m.in.:
        a. utrata bądź ubytek wartości ubezpieczonego sprzętu nastąpiły z powodu jego zniszczenia lub uszkodzenia w wyniku nieprzewidzianego wypadku uniemożliwiającego dalsze spełnianie zamierzonych funkcji.
        b. utrata sprzętu nastąpiła wskutek kradzieży z włamaniem, rabunku, dewastacji i wandalizmu.

2) Do szkód objętych ubezpieczeniem zalicza się m.in. szkody wynikłe w następstwie:
   a. działania człowieka:
      a. niewłaściwej obsługi sprzętu, tj. nieostrożności, zaniedbania, niewłaściwego użytkowania,
      b. braku kwalifikacji, błędu operatora itp.;
      c. świadomego i celowego zniszczenia przez osoby trzecie, pracowników i współpracowników ubezpieczającego (jednak z zastosowaniem klauzuli reprezentantów),
   b. kradzieży z włamaniem, rabunku, wandalizmu i dewastacji. Ubezpieczyciel ponosi odpowiedzialność także za szkody powstałe wskutek kradzieży z pojazdu lub kradzieży całego pojazdu wraz ze sprzętem.
   c. ognia (w tym działania dymu, sadzy itp.) oraz polegające na osmaleniu, przypaleniu, a także w wyniku wszelkiego rodzaju eksplozji, implozji, uderzenia piorunu bezpośrednio i pośrednio na przedmiot ubezpieczenia, upadku statku powietrznego oraz w akcji ratunkowej
   d. wody, powodzi, wylewu wód podziemnych, a także czynników atmosferycznych w postaci mrozu, śniegu, deszczu wilgoci, pary wodnej itp.
   e. wiatru, gradu, lawiny, obsunięcia i zapadania się ziemi, huraganu, trzęsienia ziemi,
   f. zbyt wysokiego lub zbyt niskiego napięcia albo całkowitego zaniku napięcia w sieci instalacji elektrycznej, szkód przepięciowych i pochodnych powstałych w związku z uderzeniem pioruna,
   g. sprzęt elektroniczny ubezpieczony jest również w zakresie szkód spowodowanych przez upadek.
3) Dodatkowe rozszerzenie dotyczące ochrony sprzętu nie podłączonego na stanowisku pracy lub podczas przerwy w eksploatacji.

4. Miejsce instalacji sprzętu i oprogramowania/systemu.

- Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu, w budynkach urzędu lub budynkach jednostek podległych, w miejscach wskazanych przez Zamawiającego.

5. Zestawienie zakresu dostaw i usług.

Lp.	Nazwa	Wymagana minimalna długość gwarancji (m-ce)	Ilość	Jednostka miary	Uwagi
1.	Serwer	12 (kryterium oceny)	2	Szt.	Wnioskodawca obecnie posiada przestarzałe serwery poza okresem gwarancji. Konieczny jest zakup dwóch serwerów, które utworzą wydajny klaster i posłużą jako podstawa do uruchomienia na klastrze maszyn wirtualnych przeznaczonych dla poszczególnych systemów dziedzinowych. Parametry serwerów: 2 procesory, 256 GB RAM, zasilacz min. 800W.
2.	Macierz dyskowa	12 (kryterium oceny)	1	Szt.	Pozycja dotyczy zakupu macierzy dyskowej, produkcyjnej, na której składowane i przetwarzane będą dane systemów dziedzinowych pozwalających na świadczenie e-usług i pracę zdalną. Parametry urządzenia: 2 kontrolery dostępowe 2-portowe, 18 dysków SSD SAS min.1,9 TB.
3.	Oprogramowanie do wirtualizacji	12 (kryterium oceny)	1	Szt.	Oprogramowanie do wirtualizacji niezbędne do stworzenia dedykowanego klastra niezawodnościowego na rozbudowywanych serwerach. Oprogramowanie konieczne do zapewnienia warunków pracy zdalnej i świadczenia e-usług publicznych przez gminę.
4.	Oprogramowanie do backupu	12 (kryterium oceny)	1	Szt.	Oprogramowanie do backupu pozwoli na wykonywanie kopii zapasowych danych oraz całych maszyn wirtualnych. Będzie zainstalowane na serwerze do wykonywania kopii. Koszt pozycji uwzględnia licencje dla 4 CPU (2 serwery wirtualizacyjne).
5.	System domenowy	wieczysta	1	Szt.	Kalkulacja pozycji uwzględnia koszt 2 systemów operacyjnych niezbędnych do funkcjonowania serwerów wirtualizacji i backupu oraz koszty licencji dostępowych (CAL) dla użytkowników (100 licencji). Zakup jest niezbędny do zapewnienia dostępu i

					funkcjonowania całej planowanej infrastruktury.
6.	Firewall	12 (kryterium oceny)	1	Szt.	W ramach pozycji zaplanowano zakup urządzenia typu firewall (UTM) będącego centralną zaporą sieciową i pozwalającego na zarządzenia całym ruchem w obrębie sieci JST. Pozwalającego na zarządzanie ruchem sieciowym, wyposażonego w złącza 10G. UTM będzie głównym urządzeniem odpowiedzialnym za bezpieczeństwo informatyczne urzędu i umożliwiającym pracę zdalną i zdalne połączenia dla pracowników jednostki.
7.	Przełączniki CORE	12 (kryterium oceny)	2	Szt.	Przełącznik sieciowy jest elementem sieci niezbędnym do prawidłowej jej pracy w urzędzie. Urządzenia pozwolą na połączenie serwerów wirtualizacyjnych z macierzą dyskową i ich udostępnienie na zewnątrz dla urzędników. Zaplanowano zakup urządzenia o parametrach min. min. 24 porty 10G.
8.	Przełącznik IDF	12 (kryterium oceny)	2	Szt,	Projekt zakłada zakup dwóch przełączników sieci LAN-IDF. Urządzenia 24 portowe Gigabit Ethernet (10/100/1000) z 4 portami uplink 10G SFP+ pozwolą na połączenie urządzeń sieciowych z różnych lokalizacji Gminy do jednej centralnej serwerowni oraz zapewnią dostęp do sieci LAN użytkownikom, pracownikom gminy (komputery).
9.	Stacje robocze	12 (kryterium oceny)	13	Szt.	Pozycja dotyczy komputerów z systemem operacyjnym oraz oprogramowaniem do pracy biurowej. Typ AIO; 24 cale, 8 GB RAM, 256 SSD.
10.	Monitory	12 (kryterium oceny)	15	Szt.	W pozycji przewidziano zakup monitorów przeznaczonych dla pracowników urzędu. Monitory będą przeznaczone do współpracy z zakupywanymi laptopami oraz z innymi jednostkami roboczymi posiadanymi już przez JST. Pozwolą na poprawę komfortu pracy urzędników i ułatwią zdalną obsługę mieszkańców.

					Zaplanowano zakup urządzeń o przekątnej min. 24 cale, rozdzielczość FHD.
11.	Laptopy	12 (kryterium oceny)	7	Szt.	Pozycja uwzględnia koszt zakupu laptopa dla pracowników urzędu – służby informatyczne. Urządzenia pozwolą na pracę zdalną w przypadku pandemii, zdalną obsługę systemów, programowanie. Parametry planowane: komputer do zastosowań zaawansowanych, min. 16 GB RAM, min. 256 GB SSD, system operacyjny, pakiet biurowy – licencja wieczysta.
12.	Urządzenia UPS dla jednostek	12 (kryterium oceny)	2	Szt.	Urządzenia UPS są krytycznym elementem bezpieczeństwa informatycznego. Umożliwiają podtrzymanie zasilania dla serwerów i innych urządzeń krytycznych sieci do czasu przejścia na zasilanie awaryjne lub bezpiecznego wyłączenia systemów bez utraty danych. Planowane w pozycji urządzenia przeznaczone są do ochrony sieci w jednostkach podległych gminy. Zaplanowano urządzenia o mocy min. 2000V/1600W.
13.	Urządzenie NAS	12 (kryterium oceny)	3	Szt.	Pozycja uwzględnia koszt zakupu urządzeń NAS przeznaczonych dla jednostek wydzielonych. Urządzenia będą służyły jako miejsce wykonywania kopii zapasowych oraz jako miejsce na przechowywanie plików współdzielonych. Pozwolą tez na zdalny dostęp do swoich zasobów umożliwiając pracę zdalną pracownikom. Zaplanowano zakup urządzeń wyposażonych w min.2 dyski pozwalających na konfiguracje w RAID1.
14.	Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.	12	1	Szt.	Kalkulacja obejmuje koszty usług informatycznych w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego i oprogramowania zakupionych w ramach projektu, związanych z wdrożeniem platformy sprzętowej (wirtualizacyjnej), migracją danych z dotychczasowych urządzeń,

					ustaleniem i skonfigurowaniem zasad bezpieczeństwa sieciowego, montaż urządzeń, instruktaż z zakresu wdrożonych rozwiązań dla służb informatycznych w urzędzie. Dla całości usług przewidziano 135 godz., w tym: Instalacja urządzeń serwerowych i komputerowych – 35 godz. Migracja danych – 20 godz. Konfiguracja całego systemu wirtalizacyjnego – 30 godz. Konfiguracja polityk sieciowych i bezpieczeństwa – 30 godz. Testy systemu – 10 godz.

6. Szczegółowy opis pozycji.

6.1. Serwer – szt.2 – wymagania minimalne

Lp.	Parametr lub warunek	Minimalne wymagania
1	Obudowa	-Typu Rack, wysokość maksimum 1U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack;
2	Płyta główna	-Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych; -wyposażona w minimum 32 gniazda pamięci RAM DDR4, obsługa do 4000GB pamięci RAM DDR4 3200 MHz i do 10000GB pamięci RAM DDR4 i Optane PMem -Minimum 3 złącza PCI Express generacji 4, o prędkości x16; -Wszystkie złącza PCI Express muszą być aktywne; -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania klatek dyskowych serwera); -Zainstalowany moduł TPM 2.0 posiadający wsparcie dla systemu operacyjnego Windows Server 2022;
3	Procesory	Zainstalowane dwa procesory 8-rdzeniowe w architekturze x86, osiągające wynik w testach wydajności SPECrate2017_int_base min. 125 pkt. przy konfiguracji z dwoma procesorami dla dowolnej platformy dwuprocesorowej producenta serwera, który jest oferowany w postępowaniu przez oferenta. Wymagamy aby był załączony PDF ze strony spec.org i poświadczony przez producenta serwera oferowanego w postępowaniu; Nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych;
4	Pamięć RAM	-Zainstalowane 256 GB pamięci RAM typu DDR4 Registered, 3200Mhz w kościach o pojemności 32GB; -Wsparcie dla technologii zabezpieczania pamięci ECC, Memory Scrubbing, SDDC lub równoważnej; -Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM (memory mirror);
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler RAID SAS 12Gb/s , obsługujący RAID 0, 1, 5, 10, 50;
6	Dyski twarde	-Zainstalowane 2 dyski SSD o pojemności 240GB każdy, dyski hot-plug, DWPD min. 1,5; -Minimum 4 wnęki dla dysków Hotplug 3,5 cala,
7	Inne napędy zintegrowane	-Brak
8	Kontrolery LAN	-Dwie osobne karty sieciowe LAN, 4x1Gbit/s oraz 2x 10Gbit/s SFP+ , niezajmujące slotu PCI Express (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express); -Porty 10Gb/s SFP+ wyposażone w moduły światłowodowe MM;
9	Kontrolery I/O FC/SAS/Inne	-Jedna dwuportowa karta FC 16Gb/s wyposażona w moduły światłowodowe.
10	Porty	-zintegrowana karta graficzna ze złączem VGA z tyłu serwera; -2x USB 3.0 dostępne na froncie obudowy -2x USB 3.0 dostępne z tyłu serwera -1x USB 3.0 wewnątrz serwera Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;
11	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug o mocy maksymalnej 500W, o sprawności 94% (tzw klasa Platinum); -Redundantne wentylatory hotplug; -Serwer dostarczony wraz z dwoma kablami C13-C14 o długości min. 2,5m każdy;

12	Zarządzanie	-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zarządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera. Wymaga się aby system rozpoznawania awarii był niezależny od zasilania i działał (wskazywał uszkodzony element) po odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym). -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera) • Możliwość pobrania darmowego oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera, umożliwiającego konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). • Zainstalowana, dedykowana dla potrzeb karty zarządzającej pamięć flash o pojemności minimum 16 GB; • Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); • Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; • Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; • Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; • Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory,

		kontrolery RAID, karty rozszerzeń); • Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; • karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera;
13	Wspierane OS	-VMWare 6.7 U3, VMware 7.0 U2;
14	Gwarancja	-7 lat gwarancji producenta serwera w trybie onsite z gwarantowanym czasem skutecznej naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Fixtime); -Uszkodzone dyski pozostają u Zamawiającego; -Dostępność części zamiennych co najmniej przez 5 lat od momentu zakupu serwera; -Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji; -Wymagana możliwość automatycznego powiadamiania o awarii serwera centrum serwisowego producenta. Jeżeli funkcja taka jest płatna należy ten koszt uwzględnić w ofercie.
15	Dokumentacja, inne	-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty). -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Unii Europejskiej. Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg; -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu w języku polskim lub angielskim; -Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne; -Wymagane jest oświadczenie Producenta oferowanego serwera, iż wymagany w postepowaniu poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta serwera na potrzeby oferty w niniejszym postępowaniu; -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; -Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia.

		Zamawiający nie dopuszcza dostosowywania funkcji na potrzeby niniejszego postępowania. -Wszystkie parametry i funkcje oferowanego serwera muszą być potwierdzone w ogólnodostępnej dokumentacji producenta.

6.2. Macierz dyskowa – szt. 1 – wymagania minimalne

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
1.	Obudowa	1) Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych HDD i/lub dysków SSD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych, kontrolujących wszystkie zasoby dyskowe macierzy z poziomu pojedynczej konsoli WebGUI/CLI administratora; 2) Macierz musi posiadać architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez kontrolery i dyski dla zapisów danych Użytkownika; 3) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie; 4) Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia); 5)Każdy moduł/obudowa macierzy powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii; 6) Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy; 7) Moduły dla dalszej rozbudowy o dodatkowe dyski i przestrzeń dyskową muszą zapewniać gęstości upakowania co najmniej 24 dysków 2,5” lub co najmniej 12 dysków 3,5” na każde 2U przestrzeni instalacyjnej w szafie przemysłowej rack standardu 19”; 8) Dostarczona konfiguracja macierzy musi pozwalać na połączenie kaskadowe lub w układzie pętli pomiędzy modułami rozwiązania (moduł kontrolerów, moduły/półki dyskowe), z wykorzystaniem minimum 2-torów kablowych w tych połączeniach – okablowanie to musi być zgodne ze standardem SAS 12Gb/s. W przypadku braku obsługi połączeń w układzie pętli dopuszcza się jako alternatywne rozwiązanie macierz z zainstalowanymi 4 kontrolerami RAID;
2.	Pojemność	1) Oferowana macierz musi obsługiwać min. 142 dyski wykonane w technologii hot-plug – jeżeli dla obsługi tej funkcjonalności konieczny jest zakup dodatkowych licencji to należy ją dostarczyć wraz z macierzą; 2) Model oferowanej macierzy musi obsługiwać przestrzeń dyskową w trybie tzw. surowym (RAW) minimum 4000 TB, bez konieczności wymiany zainstalowanych kontrolerów – wymagana zgodność z zapisami aktualnej na moment składania oferty specyfikacji technicznej macierzy, udostępnionej publicznie na stronie internetowej producenta lub jego przedstawiciela w Polsce; 3) Model oferowanej macierzy musi umożliwiać rozbudowę do wyższego modelu z tej samej rodziny urządzeń w trybie w „data-in-place” tj. z wykorzystaniem wszystkich modułów półek rozszerzeń dyskowych wykorzystywanych przed rozbudową i z dostępem do wcześniej zapisanych danych; 4) Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych

		jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika;
3.	Kontrolery	1) Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami; 2) Każdy z kontrolerów macierzy musi posiadać po minimum 16 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu; 3) Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 1,6 TB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie dysków SSD. Obecnie nie jest wymagana rozbudowa pamięci cache przeznaczonej do odczytu; 4) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik; 5) Kontrolery muszą posiadać możliwość ich wymiany (w przypadku awarii lub planowych zadań utrzymaniowych) bez konieczności wyłączania zasilania całego urządzenia – wymaganie w przypadku konfiguracji z min. 2 kontrolerami; 6) Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach; 7) Każdy z kontrolerów RAID powinien posiadać dedykowane minimum 2 interfejsy RJ-45 Ethernet obsługujące połączenia z prędkością minimum 1Gb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy; 8) Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej; 9) Każdy kontroler macierzy musi pozwalać na konfigurację interfejsów niezbędnych dla współpracy w sieci IP/FC/SAS SAN oraz NAS; 10) Dla obsługi operacji blokowych I/O w sieci IP/FC/SAS SAN, kontrolery macierzy muszą wspierać protokoły transmisji (komunikacja z serwerami): FC 32/16Gb/s , iSCSI 10/1Gb/s, SAS 12Gb/s; 11) Dla obsługi operacji plikowych I/O w sieci NAS kontrolery macierzy muszą wspierać minimum protokoły dostępu: CIFS, NFS. Obecnie nie jest wymagana obsługa protokołów CIFS, NFS, ale musi istnieć możliwość rozbudowy o tą funkcjonalność. Rozbudowa o tę funkcjonalność nie może wymagać montażu żadnych zewnętrznych elementów/modułów po za obudową macierzy. Przy ewentualnej rozbudowie o dostęp plikowy dopuszczana jest wymiana części z obecnie wymaganych interfejsów SAN; 12) Uruchomienie obsługi protokołów CIFS i NFS nie może powodować zmniejszenia rozmiaru pamięci podręcznej cache wykorzystywanej przez macierz do obsługi protokołów blokowych – jako równoważność dla tego wymagania dopuszczone jest skonfigurowanie dodatkowo minimum po 16GB pamięci podręcznej Cache dla każdego kontrolera lub 2 grup dyskowych RAID 1 z dyskami SAS SSD minimum 200GB – nie jest wymagane dostarczenie tej funkcjonalności w postepowaniu, możliwość rozbudowy w przyszłości; 13) Kontrolery macierzy muszą obsługiwać do 72 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów;
4.	Interfejsy	1) Oferowana macierz musi mieć minimum 4 porty FC 16Gb/s (wyposażone w moduły/wkładki światłowodowe), przeznaczone do dołączenia serwerów, wyprowadzone na każdy kontroler RAID. Wraz z macierzą należy dostarczyć min. 6 kabli światłowodowych LC-LC o długości min. 5 metrów każdy; 2) Macierz musi umożliwiać wymianę portów do transmisji danych(z serwerami) na porty obsługujące protokoły: FC 32 Gb/s, iSCSI 10Gb/s, iSCSI 1Gb/s, SAS 12Gb; 3) Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencją na instalację i obsługę

		każdego z wymienionych protokołów transmisji danych;
5.	Poziomy RAID	1) Macierz musi zapewniać poziom zabezpieczenia danych na dyskach, definiowany poziomami RAID: 0, 1, 10, 5 , 50, 6;
6.	Wspierane dyski	1) Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex; 2) Oferowana macierz musi wspierać dyski hot-plug: - dyski elektroniczne SSD i mechaniczne HDD iż interfejsami SAS12Gb/s; - dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm oraz 15k rpm; 3) Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD zainstalowanych w pojedynczej obudowie o wysokości 2U; 4) Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5” i 3,5”; 5) Macierz musi obsługiwać min. 72 dyski SAS SSD w całym rozwiązaniu; 6) Wymagane jest dostarczenie macierzy zawierającej min. 18 dysków SSD-SAS o pojemności min. 1,92 TB każdy; 7) Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach: - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID - hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID; 8) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess); 9) Dostarczona macierz w oferowanej konfiguracji umożliwia szyfrowanie danych na zainstalowanych dyskach dowolnego typu – funkcjonalność realizowana bezpośrednio przez kontrolery macierzy dla danych blokowych – minimum AES 256. Jeżeli funkcjonalność ta wymaga dodatkowych elementów sprzętowych bądź aktywacji dodatkowej licencji to należy dostarczyć je wraz z rozwiązaniem dla maksymalnej pojemności macierzy.
7.	Opcje software’owe	1) Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 1024 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanej macierzy; 2) Macierz musi umożliwiać zdefiniowanie min. 4096 woluminów (LUN); 3) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy; 4) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową; 5) Macierz musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server 2012R2/2016/2019, SuSE Linux, Oracle Linux, Oracle VM, RedHat Linux, AIX, Solaris, VMWare , Citrix XEN Server. 6) Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem); 7) Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI (w zależności od zastosowanych portów), bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 8) Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication;

		9) Replikacja danych jak w pkt.7 musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych; 10) Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 11) W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów; 12) Macierz musi obsługiwać dla interfejsów iSCSI i interfejsów obsługujących protokoły CIFS i NFS adresacje IP v.4 i IP v.6; 13) W przypadku korzystania z protokołów dostępu plikowego obsługa CIFS i NFS musi odbywać się jednocześnie; 14) Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy; 15) Model oferowanej macierzy musi wspierać rozwiązania klasy 'klastra macierzowego' tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami ; 16) Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI (w zależności od zastosowanych portów), zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 17) Pod użytym w pkt. 15 pojęciem 'wysoka dostępność zasobów dyskowych' należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej; 18) Dla uruchomienia funkcjonalności 'klastra macierzowego' musi być możliwość wykorzystania istniejącej infrastruktury FC/IP SAN Użytkownika w zakresie przełączników FC/Ethernet i kart HBA FC/Ethernet zainstalowanych w serwerach Użytkownika; 19) Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie 'klastra macierzowego', musi wspierać poziomy RAID1, RAID10, RAID5, RAID6 bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną; 20) Funkcjonalność 'klastra macierzowego' musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover); 21) Funkcjonalność 'klastra macierzowego' musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover); 22) Funkcjonalność 'klastra macierzowego' musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback); 23) Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 24) Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SAS, NLSAS; 25) Macierz musi pozwalać na definiowanie minimum 32 różnych polityk i zasad migrowania danych w obrębie tej samej macierzy; 26) Maksymalna wielkość pojedynczego bloku danych podczas migracji i realokacji mechanizmami AST nie może przekraczać 256MB;

		27) Mechanizm AST musi być wyposażony w funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 28) Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny; 29) Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O; 30) Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN;
8.	Konfiguracja, zarządzanie	1) Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI, SAS) jak i do obsługi transmisji protokołami CIFS/NFS; 2) Oprogramowanie zarządzające musi być dostarczone w wariancie dla maksymalnej obsługiwanej pojemności dyskowej macierzy oraz dla maksymalnej liczby dysków wspieranej przez oferowaną macierz; 3) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. 4) Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora; 5) Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI ;
9.	Gwarancja i serwis	1) Macierz dyskowa musi zostać objęta gwarancją producenta w trybie onsite, z czasem reakcji w miejscu instalacji sprzętu, najpóźniej w następnym dniu roboczym od zgłoszenia usterki. Producent macierzy musi umożliwiać skuteczne zgłaszanie usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne; 2) Macierz musi być zaoferowana z serwisem producenta macierzy, który w przypadku wymiany dysków twardych HDD/SSD, umożliwia pozostawienie wszystkich uszkodzonych nośników u Zamawiającego; 3) Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia, w ciągu 60 miesięcy od daty zakupu; 4) Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy; 5) Macierz musi umożliwiać konfigurację i uruchomienie dedykowanej funkcji automatycznego powiadomienia serwisu o usterce przez samo urządzenie (poprzez dedykowany system wbudowany w macierz - bez pośrednictwa administratora, nie dopuszcza się użycia ogólnodostępnych mechanizmów - poczty email w tym m.in. protokołu SNMP i SMTP, nie dopuszcza się SMS – Zamawiający nie dopuszcza możliwości komunikacji z/do macierzy poprzez pocztę email/SNMP/SMTP itp. z powodów bezpieczeństwa). Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy. 6) Macierz musi pochodzić z legalnego kanału sprzedaży producenta w Polsce i musi reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych;

		7) Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia; 8) Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje;

6.3. Oprogramowanie do wirtualizacji – 1 szt. - wymagania minimalne

Wraz ze sprzętem należy dostarczyć oprogramowanie do wirtualizacji. Dostarczane oprogramowanie musi być w najnowszej wersji obecnie dostępnej na rynku.

Licencja dla 3 serwerów fizycznych posiadających 2 procesory ze wsparciem technicznym 9x5 z 4h-czasem zdalnej reakcji oraz gwarancją utrzymania aktualnej wersji przez zaoferowany czas gwarancji.

Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.

- Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
- Pojedynczy klaster może się skalować do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
- Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 768 logicznych wątków oraz do 12TB pamięci fizycznej RAM.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-256 procesorowych.
- Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
- Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
- Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 11, SLES 12, SLES 15, RHEL 8, RHEL 7, RHEL 6, RHEL 5, RHEL 4, Solaris 11 ,Solaris 10, Debian, CentOS, FreeBSD, Asianux, Ubuntu 20, Ubuntu 18, Ubuntu 10, SCO OpenServer, SCO Unixware, Mac OS X, Amazon Linux 2, Oracle Linux.
- Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
- Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
- Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.
- Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
- Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez

przerywania ich pracy.

- Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
- Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
- Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.
- System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
- Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
- Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
- Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
- Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

6.4. Oprogramowanie do backupu – szt.1 – wymagania minimalne

Wymagania ogólne

Minimalna ilość licencji musi umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 30 VM oraz 4 serwerów fizycznych.

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej

Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.

Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.

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.

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 (tzw. reverse-inremental)

Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji

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 pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.

Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania

Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.

Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)

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. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji

Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania

Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)

Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO

Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej

Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych

Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora

Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn

Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)

Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.

Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.

Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)

Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik

Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)

Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

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 i Hyper-V 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. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami

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 umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.

Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:

- Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
- BSD: UFS, UFS2
- Solaris: ZFS, UFS
- Mac: HFS, HFS+
- Windows: NTFS, FAT, FAT32, ReFS
- Novell OES: NSS

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.

Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),

Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych

Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych

Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.

Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem

Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere

Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

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 monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie

System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware

System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter

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 w formacie HTML oraz Excel

System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk

System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora

System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów

System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)

System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna

System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego

System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta

System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.

System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware

System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x

Raportowanie

System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022

System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.

System musi być certyfikowany przez VMware i posiadać status „VMware Ready”

System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V

System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF

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 i dostarczania ich do odbiorców w określonych przez administratora interwałach

System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów

System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych

System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych

System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury

System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta

System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.

System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)

System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

6.5. System domenowy – szt.1 (komplet) – wymagania minimalne

Licencje na serwerowy system operacyjny – szt. 3

Licencje na serwerowy system operacyjny muszą uprawniać do zainstalowania serwerowego systemu operacyjnego na 3 oferowanych serwerach fizycznych lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego na każdym z 3 oferowanych serwerów fizycznych. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanych serwerach.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4) 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.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9) 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).
10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18) 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),
19) 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.
20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25) 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 8.1.
    c) Zdalna dystrybucja oprogramowania na stacje robocze.
    d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,
        iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f) Szyfrowanie plików i folderów.
    g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    i) Serwis udostępniania stron WWW.
    j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
    k) Wsparcie dla algorytmów Suite B (RFC 4869),
    l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
        i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
        ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
        iii. Obsługi 4-KB sektorów dysków

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) 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.
27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Licencje dostępowe:
Wymaga się aby oferowane licencje dla systemu operacyjnego umożliwiały korzystanie z zasobów dla 100 użytkowników (100 licencji dostępowych).

6.6. Firewall (UTM) – szt. 1 – wymagania minimalne.

Wymagania Ogólne
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
5. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:
W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Analiza ruchu szyfrowanego protokołem SSH.
13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

14. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
15. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
16. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
17. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
18. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure
    - Google Cloud Platform (GCP).

- OpenStack.
- VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria

producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

6.7. Przełącznik CORE – szt. 2. – wymagania minimalne

Przełącznik wielowarstwowy L2/L3, zarządzany

Typ i liczba portów: 12 portów 10GBaseT i 12 portów SFP+
Porty SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:

- Gigabit Ethernet 1000Base-SX
- Gigabit Ethernet 1000Base-LX/LH
- 10Gigabit Ethernet 10GBase-SR
- 10Gigabit Ethernet 10GBase-LR
- 10Gigabit Ethernet typu twinax

Port konsoli USB Type-B/RJ45
Porty dostępowe przełącznika zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

Parametry wydajnościowe:

- Przepustowość przełącznika (switching bandwidth) 238 Gb/s
- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów 320 Mpps
- Pamięć DRAM – 512 MB
- Pamięć flash – 256 MB
- Procesor wbudowany 1,3 GHz
- Wielkość bufora pakietów - 3 MB
- 4 000 grup IGMP
- 32 grupy połączeń zagregowanych typu „port channel" LACP
- 8 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP
- 2 000 wpisów w listach kontroli dostępu ACL
- 8 kolejek sprzętowych

Obsługa:

- 4 096 aktywnych sieci VLAN
- 32 000 adresów MAC
- 7 100 statycznych tras IPv4
- 256 interfejsów L3

Obsługa ramek Ethernet Jumbo 9 000 B

Możliwość łączenia do 8 jednostek w stos poprzez porty 10 GE, zarządzane jako jeden system z funkcją failover active/standby
Funkcjonalność cross-stack QoS, VLAN, LAG i port mirroring

Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

- IEEE 802.1w Rapid Spanning Tree
- Per-VLAN Rapid Spanning Tree (PVRST+)
- IEEE 802.1s Multi-Instance Spanning Tree
- Obsługa 126 instancji protokołu STP

Funkcje wirtualnej sieci LAN: Voice VLAN, Protocol based VLAN
Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
Protokół rejestracji GARP VLAN (GVRP)

Mechanizmy związane z bezpieczeństwem sieci:

- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
- Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez

suplikanta 802.1X
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,\
- Obsługa HTTPS, SSH, SSL
- Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP)

Mechanizmy związane z zapewnieniem jakości usług w sieci:
- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
- Implementacja algorytmu Weighted Round Robin dla obsługi kolejek
- Możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi,
- Kontrola sztormów dla ruchu broadcast/multicast/unicast
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

Obsługa standardów komunikacyjnych:
IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet

Obsługa protokołu NTP
Funkcje DHCP server, DHCP relay
Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snooping
Blokowanie Head of Line (HOL)

Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD)
Zapobieganie atakom DoS

Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6
Routing dynamiczny RIP v2

Zarządzanie
- Port konsoli
- Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
- Obsługa protokołów SNMPv3, SSHv2, https, syslog
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia
- Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
- Obsługa protokołu LLDP i LLDP-MED

Obsługa funkcji Plug & Play
Przycisk reset
Certyfikaty: UL 60950, FCC 15 A, CSA 22.2, CE mark lub równoważne

Zasilanie 230V AC
Wysokość maksymalnie 1U, montowany w szafie typu RAC 19''

6.8. Przełącznik IDF – szt. 2 – wymagania minimalne.

Urządzenia sieciowe i osprzęt sieciowy pozwalający na przyłączenie do szerokopasmowego Internetu.
Przełącznik wielowarstwowy L2/L3, zarządzany

Typ i liczba portów:
Min. 24 porty 10/100/1000BaseT RJ-45, min. uplink 4x10G SFP+
Porty SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:

- Gigabit Ethernet 1000Base-SX
- Gigabit Ethernet 1000Base-LX/LH
- 10Gigabit Ethernet 10GBase-SR
- 10Gigabit Ethernet 10GBase-LR
- 10Gigabit Ethernet typu twinax

Port konsoli USB Type-B/RJ45
Porty dostępowe przełącznika musza być zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

Parametry wydajnościowe:

- Przepustowość przełącznika (switching bandwidth) min. 125 Gb/s
- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów min. 95 Mpps
- Pamięć DRAM – min. 512 MB
- Pamięć flash – min. 256 MB
- Wielkość bufora pakietów – min. 1,5 MB
- Min. 255 grup IGMP
- Min. 4 grupy połączeń zagregowanych typu „port channel" LACP
- Min. 8 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP
- Min. 512 wpisów w listach kontroli dostępu ACL
- Min. 8 kolejek sprzętowych

Obsługa:

- Min. 255 aktywnych sieci VLAN
- Min. 8 000 adresów MAC
- Min. 32 statyczne trasy IPv4
- Min. 16 interfejsów L3
- ramek Ethernet Jumbo 9 000 B

Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

- IEEE 802.1w Rapid Spanning Tree
- Per-VLAN Rapid Spanning Tree (PVRST+)
- IEEE 802.1s Multi-Instance Spanning Tree
- Obsługa 126 instancji protokołu STP

Przełącznik musi wspierać:

- obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
- protokół rejestracji GARP VLAN (GVRP)

Przełącznik musi wspierać mechanizmy związane z bezpieczeństwem sieci:

- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
- Autoryzacja użytkowników w oparciu o IEEE 802.1X
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
- Obsługa HTTPS, SSH, SSL,

- Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP)

Przełącznik musi wspierać mechanizmy związane z zapewnieniem jakości usług w sieci:
- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
- Implementacja algorytmu Weighted Round Robin dla obsługi kolejek
- Możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi,
- Kontrola sztormów dla ruchu broadcast/multicast/unicast
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

Przełącznik musi wspierać obsługiwać standardy komunikacyjne:
IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet

Obsługa protokołu NTP
Funkcje DHCP server, DHCP relay
Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snooping
Blokowanie Head of Line (HOL)

Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD)
Zapobieganie atakom DoS

Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6

Zarządzanie
- Port konsoli
- Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
- Obsługa protokołów SNMPv3, SSHv2, https, syslog
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia
- Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
- Obsługa protokołu LLDP i LLDP-MED
- Obsługa funkcji Plug & Play
- Przycisk reset

Inne
- Zasilanie 230V AC
- Wysokość maksymalnie 1U, montowany w szafie typu RAC 19''

6.9. Stacje robocze - szt. 13 – wymagania minimalne

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Komputer All in One, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
2.	Matryca	- Zintegrowana w jednej obudowie z PC - Typ ekranu: 23.5-24”

		- Jasność: min. 250 cd/m2 - Kontrast: min. 1000:1 - Kąty widzenia (pion/poziom): min. 178°/178° - Czas reakcji matrycy: maks. 14 ms - Kolory: min. 16.7mln - Obsługiwana rozdzielczość: min. 1920 x 1080 - Powłoka powierzchni ekranu: Przeciwodblaskowa - Zakres pochylenia względem podstawy: w nie mniejszy niż 0°-20° - Regulacja wysokości: min. 130 mm
3.	Wydajność	Procesor klasy x86 ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach biurowych, osiągający w teście wydajności (BAPCO): Sysmark 2018 – Overall Rating wynik min.1200 Productivity – co najmniej wynik 1100 punktów Creativity – co najmniej wynik 1400 punktów Responsiveness – co najmniej wynik 1200 punktów Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta.
4.	Pamięć RAM	Pamięć operacyjna: 8GB 2933 możliwość rozbudowy do min 64 GB. Jeden slot wolny.
5.	Pamięć masowa	Dysk SSD PCIe M.2 NVMe o pojemności min. 256 GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników, wspierający technologię sprzętowego szyfrowania danych.
6.	Zintegrowana karta graficzna	Wydajność grafiki: Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Obsługująca funkcje: DirectX 12, OpenGL 4.5.
7.	Sieć	Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika)
8.	Bezpieczeństwo	Złącze umożliwiające zabezpieczenie komputera przed wyniesieniem, Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Co najmniej TPM 2.0. Certyfikowane oprogramowanie producenta komputera umożliwiające – bez względu na stan czy obecność systemu operacyjnego w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego.
9.	Multimedia	Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition audio. Głośniki stereo. Porty audio wymagane zarówno na przednim, jak i na tylnym panelu obudowy. Kamera FHD chowana w obudowie. Wewnętrzny mikrofon stereo.
10.	Zasilanie	Wewnętrzny zasilacz o mocy minimum 190 W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 93%, przy obciążeniu 50%.
11.	Wymiary	Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych bez stopy monitora) nie może wynosić więcej niż

		1000mm.
12.	Obudowa	Zintegrowana z monitorem (AiO), wyposażona w min. 2 kieszenie: 1 szt. 5,25" zewnętrznie (dopuszcza się zatokę na napęd optyczny typu SLIM), 1 szt. 2,5" wewnętrzne. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością demontażu stopy. Stopa dostarczona w zestawie. Obudowa trwale oznaczona logiem producenta.
13.	BIOS	Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera; - modelu płyty głównej; - nr seryjnego komputera; - wersji BIOS (z datą); - modelu procesora wraz z informacjami o prędkości taktowania; - Informacji o ilości i obsadzeniu slotów pamięci RAM wraz z informacją o prędkości taktowania; - Informacji o dysku twardym: model oraz pojemność - MAC adresie zintegrowanej karty sieciowej - temperaturze układu graficznego - temperaturze procesora - temperaturze wewnątrz obudowy komputera - statusu karty sieciowej
14.	System operacyjny	Zainstalowany system operacyjny spełniający następujące wymagania techniczne: • dostępne dwa rodzaje graficznego interfejsu użytkownika, w tym: o klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, o dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych; • interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim; • możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; • możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; • darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; • internetowa aktualizacja zapewniona w języku polskim; • wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; • wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); • funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer; • interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;

		• możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; • zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; • zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; • zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; • funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego; • funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika; • zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi; • wbudowany system pomocy w języku polskim; • możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); • możliwość zarządzania stacją roboczą poprzez polityki – przez politykę należy rozumieć zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; • wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; • automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; • wsparcie dla logowania przy pomocy smartcard; • rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; • system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; • wsparcie dla Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; • wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; • zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; • rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową; • rozwiązanie ma umożliwiać wdrożenie nowego obrazu poprzez zdalną instalację; • graficzne środowisko instalacji i konfiguracji; • transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; • zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; • udostępnianie modemu; • oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; • możliwość przywracania plików systemowych;

		• system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.); • możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
15.	Inne	Zainstalowany pakiet biurowy spełniający następujące wymagania techniczne: a. wymagania odnośnie interfejsu użytkownika: • pełna polska wersja językowa interfejsu użytkownika, • prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; b. oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: • posiada kompletny i publicznie dostępny opis formatu, • 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. oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji; d. w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); e. do aplikacji musi być dostępna pełna dokumentacja w języku polskim; Pakiet zintegrowanych aplikacji biurowych musi zawierać: 1. Edytor tekstów, 2. Arkusz kalkulacyjny, 3. Narzędzie do przygotowywania i prowadzenia prezentacji, 4. Narzędzie do tworzenia drukowanych materiałów informacyjnych, 5. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), 6. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR; Edytor tekstów musi umożliwiać: • 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, • wstawianie oraz formatowanie tabel, • wstawianie oraz formatowanie obiektów graficznych, • wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), • automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, • automatyczne tworzenie spisów treści, • formatowanie nagłówków i stopek stron, • śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • określenie układu strony (pionowa/pozioma), • wydruk dokumentów, • wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, • pracę na dokumentach utworzonych przy pomocy posiadanego przez

		Zamawiającego oprogramowania Microsoft Word 2003 lub Microsoft Word 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, • wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem, • wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa; Arkusz kalkulacyjny musi umożliwiać: • tworzenie raportów tabelarycznych, • tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, • tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, • tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService), • obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, • tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, • wyszukiwanie i zamianę danych, • wykonywanie analiz danych przy użyciu formatowania warunkowego, • nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • formatowanie czasu, daty i wartości finansowych z polskim formatem, • zapis wielu arkuszy kalkulacyjnych w jednym pliku, • zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: • przygotowywanie prezentacji multimedialnych, • prezentowanie przy użyciu projektora multimedialnego, • drukowanie w formacie umożliwiającym robienie notatek, • zapisanie jako prezentacja tylko do odczytu, • nagrywanie narracji i dołączanie jej do prezentacji, • opatrywanie slajdów notatkami dla prezentera, • umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, • możliwość tworzenia animacji obiektów i całych slajdów, • prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, • pełna zgodność z formatami plików utworzonych za pomocą

		posiadanego przez Zamawiającego oprogramowania MS PowerPoint Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: • tworzenie i edycję drukowanych materiałów informacyjnych, • tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów, • edycję poszczególnych stron materiałów, • podział treści na kolumny, • umieszczanie elementów graficznych, • wykorzystanie mechanizmu korespondencji seryjnej, • płynne przesuwanie elementów po całej stronie publikacji, • eksport publikacji do formatu PDF oraz TIFF, • wydruk publikacji, • możliwość przygotowywania materiałów do wydruku w standardzie CMYK; Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b) przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, c) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, d) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, e) automatyczne grupowanie poczty o tym samym tytule, f) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, g) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, h) mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, i) zarządzanie kalendarzem, j) udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, k) przeglądanie kalendarza innych użytkowników, l) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, m) zarządzanie listą zadań, n) zlecanie zadań innym użytkownikom, o) zarządzanie listą kontaktów, p) udostępnianie listy kontaktów innym użytkownikom, p) przeglądanie listy kontaktów innych użytkowników, q) możliwość przesyłania kontaktów innym użytkowników.
16.	Normy i standardy	Komputery mają spełniać normy i posiadać deklaracje zgodności w zakresie: -Deklaracja zgodności CE (lub równoważne np.: EPAT) Certyfikaty te mają na celu wykazanie, iż producent na etapie wytworzenia produktu podjął się spełnienia wyższych wymagań ze względu na aspekty środowiskowe, zdrowotne i ergonomie, a tym między innymi dotyczące: 1. Wydajności energetycznej 2. Bezpieczeństwa promieniowania i emisji elektromagnetycznej (testowanie produktów pod względem bezpieczeństwa podzespołów elektrycznych i emisji elektro-magnetycznej) 3. Żywotności produktu (wydłużone normy czasowe dla bezawaryjnej pracy) 4. Systemu zarządzania środowiskiem 5. Odpowiedzialności społecznej za warunki pracy (programy CSR – Corporate Social Responsibility Społecznej Odpowiedzialność biznesu – włączając EICC (wspieranie praw pracowniczych) i SA8000 (lub równoważne) – standardu certyfikacji opierający się na normach dotyczących praw człowieka, audyt warunków pracy)

		6. Zmniejszenia występowania niebezpiecznych substancji (kadm, rtęć, ołów i chrom sześciowartościowy) 7. Designu oraz recyclingu (bezpieczeństwa utylizacji produktu) 8. Ergonomiki i przystosowania produktu przyjaznego w użytkowaniu (kąty widzenia, ostrość i kontrast, właściwości akustyczne). -Być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001 (lub równoważne) -Posiadać certyfikat TCO Certified All-in-One PC 8 (lub równoważne) -Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 w pozycji operatora w trybie jałowym (IDLE) wynosząca maksymalnie 18 dB(A) (lub równoważne)
17.	Porty i złącza	- 1 x Display Port - 1 x Audio: line-in - 1 x Audio: line-out - 1 x Audio: słuchawki z przodu obudowy - 1 x RJ45 (karta sieciowa) - 7 szt. USB w tym: minimum 3 porty z przodu obudowy (w tym min. 2x USB 3.2 gen1 typ A oraz min. 1x USB 3.2 gen1 typ C), minimum 4 porty z tyłu obudowy (w tym min. 1x USB 3.2 gen1 typ A). Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. Płyta główna: - minimum dwa złącza pamięci RAM z obsługą do 64 GB pamięci - min. 2 złącza SATA 3.0 (6 Gbit) NCQ, - co najmniej jedno złącze M.2-2280 (SSD NVMe), - co najmniej jedno złącze M.2-2230 (WLAN).
18.	Klawiatura	Klawiatura USB w układzie polski programisty, 104 klawisze – trwale oznaczona logo producenta jednostki centralnej
19.	Mysz	Mysz optyczna USB z trzema klawiszami oraz rolką (scroll) – trwale oznaczona logo producenta jednostki centralnej
20.	Gwarancja	Gwarancja jakości producenta świadczona w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta, lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca, Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta oferowanego komputera Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela Zgłoszenia serwisowe w języku polskim: • Na dedykowaną infolinie producenta komputera oraz na dedykowany adres email. • Poprzez formularz zgłoszeniowy online dostępny na stronie producenta komputera

6.10. Laptop – szt. 7 – wymagania minimalne

Lp.	Nazwa podzespołu	Minimalne wymagane parametry
1.	Zastosowanie	Zastosowanie: Komputer przenośny, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.

2.	Przekątna i rozdzielczość ekranu	Ekran o przekątnej 15,6" o rozdzielczości FHD WLED (1920x1080) i jasności co najmniej 250 cd/m2, matryca matowa AG. Metalowe, wzmacniane zawiasy.
3.	Wydajność	Procesor zaprojektowany do pracy w komputerach biurowych, osiągający w teście wydajności (BAPCO): Sysmark 2018 – Overall Rating wynik min.1200 Productivity – co najmniej wynik 1200 punktów Creativity – co najmniej wynik 1200 punktów Responsiveness – co najmniej wynik 1200 punktów Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta. Lub równoważnie, Procesor klasy x86_64 ze zintegrowaną grafiką, zapewniający równoważną wydajność całego oferowanego laptopa (Rating) min. 7500 pkt w teście Passmark CPU Mark 10 wg wyników dostępnych na stronie: https://www.cpubenchmark.net/high_end_cpus.html Wynik nie starszy niż 3 miesiące od daty publikacji postępowania.
4.	Pamięć RAM	Pamięć operacyjna: 8 GB z możliwością rozbudowy do min 64 GB, możliwość łatwej wymiany pamięci po odkręceniu pojedynczej śruby – bez konieczności demontowania laptopa. Przynajmniej jeden slot do rozbudowy pamięci RAM wolny.
5.	Pamięć masowa	Parametry pamięci masowej: dysk SSD M.2 NVMe o pojemności min. 256GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.
6.	Karta graficzna	Wydajność grafiki: Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 1,5 GB pamięci. Obsługująca funkcje: DirectX 12, OpenGL 4.4, OpenCL 2.0, HLSL shader model 5.1
7.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji)
8.	Bezpieczeństwo	Sprzętowe wsparcie technologii weryfikacji poprawności podpisu cyfrowego wykonywanego kodu oprogramowania, oraz sprzętowa izolacja segmentów pamięci dla kodu wykonywanego w trybie zaufanym wbudowane w procesor, kontroler pamięci, chipset I/O. Złącze typu Kensington Lock lub równoważne, Zintegrowany z płytą główną układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Co najmniej zgodne z TPM 2.0.
9.	Multimedia	Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki; Min. 1 cyfrowy mikrofon wbudowany w obudowie matrycy. Kamera internetowa co najmniej HD (co najmniej 720p, 30 klatek na sekundę) trwale zainstalowana w obudowie matrycy, wyposażona w diodę LED sygnalizująca działanie kamery. Wbudowany napędu optyczny w obudowę notebooka – co najmniej nagrywarka DVD-RW
10.	Klawiatura	Klawiatura wyspowa układ US –QWERTY odporna na zachlapanie, minimum 104 klawisze z wydzielonym blokiem klawiatury numerycznej.

		Touchpad wyposażony w dwa niezależne klawisze funkcyjne.
11.	Bateria i zasilanie	Min. 3-cell, 45 Wh, Li-Ion. Czas pracy na baterii minimum 10 godzin według dokumentacji producenta laptopa. Możliwość łatwej wymiany baterii po odkręceniu jeden śruby. Zasilacz o mocy min. 65 W
12.	Waga i wymiary	Waga nie więcej niż: 2 kg Grubość laptopa po złożeniu powinna być mniejsza niż 24 mm.
13.	Obudowa	Szkielet i zawiasy notebooka wykonane z wzmacnianego metalu. Możliwość wymiany pamięci RAM, dysku i baterii przez użytkownika – bez konieczności wizyty w serwisie i bez konieczności rozbierania laptopa – dostępna klapa serwisowa wymagająca odkręcenia jedynie pojedynczej śruby.
14.	Certyfikaty	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 64-bit. Deklaracja zgodności CE lub równoważne. Norma EnergyStar 8.0 - komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov oraz http://www.eu-energystar.org lub inny dokument od producenta sprzętu potwierdzający spełnianie przez oferowany sprzęt wymaganej normy. Zamawiający wymaga dodatkowo: ○ dla potwierdzenia, że oferowany sprzęt odpowiada postawionym wymaganiom i był wykonany przez Wykonawcę (a jeżeli Wykonawca nie jest producentem to przez producenta) w systemie zapewnienia jakości wg normy ISO 9001 aby Wykonawca/producent komputer posiadał: Certyfikat ISO 9001 lub inne zaświadczenie/dokument wydane przez niezależny podmiot zajmujący się poświadczaniem zgodności działań wykonawcy z normami jakościowymi - odpowiadającej normie ISO 9001. ○ Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram
15.	BIOS	Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: Modelu komputera. Nr seryjnego komputera. Wersji BIOS (z datą). Modelu procesora wraz z informacjami o prędkości taktowania. Informacji o ilości i typie pamięci RAM. Informacji o dysku twardym: producent i model oraz pojemność Informacja o napędzie optycznym (modelu napędu optycznego) MAC adresie zintegrowanej karty sieciowej Numerze matrycy Możliwość wyłączenia/włączenia bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych min.: ▪ karty sieciowej RJ45 ▪ karty sieciowej WLAN z Bluetooth ▪ kamery ▪ portów USB

		▪ czytnika kart multimedialnych ▪ kontrolera audio ▪ głośników ▪ mikrofonu ▪ zintegrowanej funkcjonalności TPM Funkcja blokowania/odblokowania BOOT-owania z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB Możliwość włączenia/wyłączenia hasła dla dysku twardego, Możliwość - bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie użytkownika, administratora i dysku twardego.
16.	Dodatkowe oprogramowanie	Oprogramowanie umożliwiające w pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu.
17.	System operacyjny	Zainstalowany system operacyjny spełniający następujące wymagania techniczne: • dostępne dwa rodzaje graficznego interfejsu użytkownika, w tym: o klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, o dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych; • interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim; • możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; • możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; • darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; • internetowa aktualizacja zapewniona w języku polskim; • wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; • zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; • wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); • funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer; • interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta; • możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; • zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; • zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; • zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe

		oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; • funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego; • funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika; • zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi; • wbudowany system pomocy w języku polskim; • możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); • możliwość zarządzania stacją roboczą poprzez polityki – przez politykę należy rozumieć zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; • wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; • automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; • wsparcie dla logowania przy pomocy smartcard; • rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; • system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; • wsparcie dla Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; • wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; • zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; • rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową; • rozwiązanie ma umożliwiać wdrożenie nowego obrazu poprzez zdalną instalację; • graficzne środowisko instalacji i konfiguracji; • transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; • zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; • udostępnianie modemu; • oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; • możliwość przywracania plików systemowych; • system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.); • możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).

18.	Oprogramowanie biurowe	Zainstalowany pakiet biurowy spełniający następujące wymagania techniczne: f. wymagania odnośnie interfejsu użytkownika: • pełna polska wersja językowa interfejsu użytkownika, • prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; g. oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: • posiada kompletny i publicznie dostępny opis formatu, • 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); h. oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji; i. w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); j. do aplikacji musi być dostępna pełna dokumentacja w języku polskim; Pakiet zintegrowanych aplikacji biurowych musi zawierać: • Edytor tekstów, • Arkusz kalkulacyjny, • Narzędzie do tworzenia i pracy z lokalną bazą danych, • Narzędzie do przygotowywania i prowadzenia prezentacji, • Narzędzie do tworzenia drukowanych materiałów informacyjnych, • Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), • Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR; Edytor tekstów musi umożliwiać: • 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, • wstawianie oraz formatowanie tabel, • wstawianie oraz formatowanie obiektów graficznych, • wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), • automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, • automatyczne tworzenie spisów treści, • formatowanie nagłówków i stopek stron, • śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • określenie układu strony (pionowa/pozioma), • wydruk dokumentów, • wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, • pracę na dokumentach utworzonych przy pomocy posiadanego przez Zamawiającego oprogramowania Microsoft Word 2003 lub Microsoft Word 2007, 2010 i 2013 i nowszego z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,

		• wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem, • wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa; Arkusz kalkulacyjny musi umożliwiać: • tworzenie raportów tabelarycznych, • tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, • tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, • tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService), • obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, • tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, • wyszukiwanie i zamianę danych, • wykonywanie analiz danych przy użyciu formatowania warunkowego, • nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • formatowanie czasu, daty i wartości finansowych z polskim formatem, • zapis wielu arkuszy kalkulacyjnych w jednym pliku, • zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013 i nowszych, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: • przygotowywanie prezentacji multimedialnych, • prezentowanie przy użyciu projektora multimedialnego, • drukowanie w formacie umożliwiającym robienie notatek, • zapisanie jako prezentacja tylko do odczytu, • nagrywanie narracji i dołączanie jej do prezentacji, • opatrywanie slajdów notatkami dla prezentera, • umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, • możliwość tworzenia animacji obiektów i całych slajdów, • prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, • pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint

		Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: • tworzenie i edycję drukowanych materiałów informacyjnych, • tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów, • edycję poszczególnych stron materiałów, • podział treści na kolumny, • umieszczanie elementów graficznych, • wykorzystanie mechanizmu korespondencji seryjnej, • płynne przesuwanie elementów po całej stronie publikacji, • eksport publikacji do formatu PDF oraz TIFF, • wydruk publikacji, • możliwość przygotowywania materiałów do wydruku w standardzie CMYK; Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: r) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, s) przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, t) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, u) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, v) automatyczne grupowanie poczty o tym samym tytule, w) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, x) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, y) mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, z) zarządzanie kalendarzem, aa) udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, bb) przeglądanie kalendarza innych użytkowników, cc) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, dd) zarządzanie listą zadań, ee) zlecanie zadań innym użytkownikom, ff) zarządzanie listą kontaktów, gg) udostępnianie listy kontaktów innym użytkownikom, hh) przeglądanie listy kontaktów innych użytkowników, ii) możliwość przesyłania kontaktów innym użytkowników.
19.	Porty i złącza	• RJ-45 (nie dopuszcza się stosowania adapterów) • Min. 1x UB 3.2 Gen2 typu USB-C z możliwością ładowania baterii laptopa oraz wyprowadzenia sygnału Display Port • Min. 3x USB 3.2 Gen1 (1 z możliwością ładowania zewnętrznych urządzeń bezpośrednio z portu USB komputera nawet przy wyłączonym laptopie). • HDMI w wersji co najmniej 1.4 • Czytnik kart multimedialnych (SD, SDHC i SDXC) • Audio: port combo mikrofon/słuchawki • Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną. • Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN obsługująca łącznie standardy IEEE 802.11ac z dwiema antenami.

		• Zintegrowana karta WLAN musi zapewniać możliwość bezprzewodowego bezpośredniego (t.j. bez pośrednictwa punktu dostępowego lub sieci LAN) podłączenia do komputera dodatkowego monitora lub projektora wyposażonego w odpowiedni adapter (lub natywną obsługę takiej funkcji) z wykorzystaniem standardów IEEE 802.11n w pasmie 2,4 GHz lub 5GHz, w trybie ekranu systemowego – z obsługą wyświetlania w trybie klonowania ekranów, rozszerzonego desktopu oraz wyświetlania ekranu systemu jedynie na dodatkowym monitorze lub projektorze (Clone, Extended Desktop, Remote Only). • Wymagana jest obsługa przesyłania dowolnej treści ekranu oraz dźwięku systemu operacyjnego z parametrami nie gorszymi niż: o rozdzielczość 1920x1080 - 30 fps–kompresja H.264 o dźwięk AC3 5.1 Surround Audio o obsługa szyfrowania WPS/WPA2/WEP • Bluetooth co najmniej w standardzie v5.0,
20.	Gwarancja	Gwarancji jakości producenta: o Świadczona w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca, o Czas reakcji NBD onsite od momentu zgłoszenia o Naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta notebooka o Zgłoszenia serwisowe drogą online (formularz online producenta notebooka), telefonicznie oraz mailem o Zamawiający wymaga oświadczenia producenta o zaoferowanym poziomie serwisowym zgodnym z wymaganym SLA

6.11. Monitory – 15 szt. – wymagania minimalne

Lp.	Parametr	Opis funkcjonalności
1.	Ekran	23,8 cala o rozdzielczości natywnej minimum 1920x1080 pikseli, maksymalny rozmiar piksela 0.275 mm, matryca matowa, pokryta powłoką 3H, technologia matrycy IPS
2.	Parametry obrazu	Odwzorowanie 16.7 miliona kolorów, kontrast typowy 1000:1, jasność min. 250 cd/m^2, czas reakcji matrycy max. 5ms, kąty widzenia pionowe/poziome minimum 178/178 stopni
3.	Wejścia wideo i inne	1x DP, 1x DVI-D, 1x D-SUB, wejście/wyjście audio
4.	Obudowa i regulacja monitora	Pochylenie ekranu w zakresie -5° / +22°(tzw. Tilt), zintegrowany zasilacz i głośniki stereo o mocy minimum 2W każdy, możliwość regulacji głośności z menu OSD monitora, złącze Kensington Lock, złącze montażu na ścianie w standardzie VESA
5.	Funkcje zarządzana energią i parametrami wyświetlania obrazu	Technologia zapewniająca zużycie energii przez monitor w trybie power save na poziomie 0.2W pozwalająca na redukcję ogólnego zużycia energii przez monitor (bez konieczności manualnego wyłączania monitora przez użytkownika), zgodność z normą Energy Star 8.0, zużycie energii przy ustawieniach EPA max. 14W
6.	Menu monitora	Regulacja głośności Regulacja jasności Regulacja kontrastu Regulacja koloru (sRGB, 5000K, 6500K, 7500K, Użytkownika (R,G,B) Menu w języku polskim oraz angielskim.
7.	Kable	kabel sygnałowy cyfrowy o długości minimum 1.8m, kabel zasilający o długości minimum 1,8m, kabel audio
8.	Certyfikaty i normy,	-Klasa energetyczna D

	dokumentacja	-TCO 8.0 -Epeat Bronze -TÜV Low Blue Light Certified -TÜV Flicker Free Certified -CE -ISO9241-307(klasa I) -RoHS, WEEE -Instrukcja obsługi monitora

6.12. Urządzenia UPS dla jednostek – 2 szt. – wymagania minimalne

1. Moc: 1600W/ 2000VA
2. Technologia True On-Line Double Conversion (VFI zg. z IEC62040)
3. Bypass automatyczny - bezprzerwowy (typu Static Switch) zapewnia nieprzerwane zasilanie odbiorników w sytuacjach krytycznych jak np.: przegrzanie lub awaria.
4. Ilość faz WE : WY – 1:1
5. Napięcie zasilające: 208 / 220 / 230 / 240 Vac
6. Zakres napięcia:
    a. 30% ÷ +30% @ 100% ≥ obc. > 80%
    b. -40% ÷ +30% @ 80% ≥ obc. > 70%
    c. -48% ÷ +30% @ 70% ≥ obc. > 60%
    d. -52% ÷ +30% @ 60% ≥ obc. > 0%
7. Częstotliwość: 50 / 60 Hz
8. Zakres częstotliwości: 20% ÷ +20%
9. THDi: <3%
10. Wejściowy współczynnik mocy: ≥0,99
11. Współczynnik mocy: 0,9
12. Regulacja napięcia statyczna/dynamiczna: ±1% / ±3%
13. Odporność na przeciążenia falownika: 110% - bez limitu, 130% - 5 min, 140% - 30 sek.,>140% - 1,5 sek.
14. Sprawność w trybie On-Line: >92%
15. Sterowane grupy gniazd – z możliwością programowego wyłączenia napięcia: 1 x 4 szt.
16. Rodzaj i ilość gniazd: IEC320-C13 x8
17. Współczynnik szczytu: 3:1
18. Czas podtrzymania (min.):
    a. - 100% obc. 4
    b. - 75% obc. 7
    c. - 50% obc. 12
1. Start z baterii: tak (tzw. zimny start) daje możliwość uruchomienia zasilacza nawet w przypadku całkowitego braku napięcia zasilającego.
2. Złącze baterii zewnętrznych: tak (Możliwość wydłużenia czasu podtrzymania przez dołożenie modułów baterii umożliwia precyzyjne dobranie wymaganego czasu autonomii.)
3. Czas ładowania: max. 4 godzin do 90% pojemności
4. Komunikacja:
    a. Standard: RS232, USB, TVSS, SNMP Slot, REPO
    b. Opcja: Karta AS-400, karta SNMP
1. Odporność na zakłócenia EN 62040-2:2006
2. Bezpieczeństwo EN 62040-1:2008 + A1:2013, CE, EN 62040-3 :2001, EN 60950-1, EN61000-3-2 :2014
3. Obudowa rack
4. Wymiary max. 2U
5. Szyny do montażu w szafie RACK 19”

6.13. Urządzenie NAS – 3 szt. wymagania minimalne

Architektura procesora: 64-bit
Częstotliwość procesora: min. Czterordzeniowy 1.4 GHz
Mechanizm szyfrowania sprzętowego: Tak
Pamięć systemowa: min. 2 GB DDR4
Ilość kieszeni na dyski: min. 2
Zgodny typ dysków:

- 3.5" SATA HDD

- 2.5" SATA HDD (with optional 2.5" Disk Holder)
- 2.5" SATA SSD (with optional 2.5" Disk Holder)

Maksymalna pojemność wewnętrzna: 24 TB (12 TB drive x 2)
Maksymalny rozmiar pojedynczego wolumenu: 108 TB
Dysk z możliwością wymiany podczas pracy (hot-swap): Tak
Porty zewnętrzne

- Port LAN RJ-45 1GbE: min 1 szt.
- Port USB 3.0: min 2 szt.

System plików

- Wewnętrzne dyski twarde EXT4
- Zewnętrzne dyski twarde:
  - EXT4
  - EXT3
  - FAT
  - NTFS
  - HFS+

6.14. Instalacja i konfiguracja – szt.1 – wymagania minimalne

Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.		
1.	**Usługi**	Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji e-usług publicznych, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. Część sprzętowa powinna zostać oparta na systemie wirtualizacji zasobów IT. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. **W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową**. Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym: a) Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia. b) Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności: i. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych.

		ii. schematy połączeń iii. mechanizmy działania głównych elementów sprzętowych: • sieć LAN • klaster wirtualizacyjny • system backupu i archiwizacji danych • system serwerowy • system macierzowy • firewall/UTM iv. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności v. sposób odbioru uzgodniony z Zamawiającym vi. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu vii. opis przypadków, w których projekt dopuszcza niedziałanie systemu viii. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia.
2.	**Montaż i fizyczne uruchomienie systemu**	**Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:** 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. 2. Rozbudowa istniejących zasobów sprzętowych. 3. Urządzenia, które nie są montowane w szafach teleinformatycznych np.: komputery, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). 10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem: a. Stworzenia połączeń sieci LAN pomiędzy przełącznikami. b. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN. c. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1.

		d. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
3.	**Instalacja i konfiguracja oprogramowania**	1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. 2. Instalacja i konfiguracja dostarczonego oprogramowania do systemu wykonywania backupu i archiwizacji danych. 3. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego). 4. Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych.
4.	**Konfiguracja przełączników sieci LAN:**	Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi lokalizacjami występującymi w projekcie według topologii gwiazdy. Centralnym punktem będzie serwerownia zlokalizowana w Urzędzie. Przełączniki LAN CORE będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego). Konfiguracja dostarczanych przełączników w zakresie: a. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. b. Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów. c. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym). d. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN. i. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink. ii. Z wykorzystaniem połączeń światłowodowych oraz miedzianych. iii. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu. iv. Należy wykorzystać wkładki o najwyższej możliwej przepustowości dla danego połączenia np.: dla portu o możliwej przepustowości 1/10Gbs (wkładka: SFP/SFP+), należy wykorzystać wkładki SFP+ o przepustowości 10Gbps. e. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN. f. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster; g. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK). h. Ustawienie serwera czasu dla urządzeń sieci LAN – przełączników sieciowych - na klaster firewall. i. Zamawiający wymaga instalacji i konfiguracji serwera logów dla urządzeń sieci LAN (maszyna wirtualna) – przełączników sieciowych, z graficznym interfejsem przeszukiwania. Zamawiający dopuszcza rozwiązania Open Source. j. Zamawiający wymaga instalacji i konfiguracji dedykowanego serwera monitorowania pracy urządzeń sieciowych z graficznym

		interfejsem przeszukiwania (maszyna wirtualna): przełączniki sieciowe, drukarki, UTM. Zamawiający dopuszcza rozwiązania Open Source. k. Wykonawcza skonfiguruje urządzenia aby raportowały, przesyłały dane do zainstalowanego serwera logów i monitorowania sieci. l. Testowanie obsługi ruchu sieciowego. m. Testowanie skuteczności zabezpieczeń.
5.	**Konfiguracja elementów bezpieczeństwa sieciowego.**	Konfiguracja urządzenia UTM w zakresie. 1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta. 3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu. 5. Konfiguracja dostarczonych systemów Firewall: a. Konfiguracja podstawowych parametrów b. Konfiguracja translacji adresów NAT c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp. d. Konfiguracja inspekcji określonych protokołów sieciowych; e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall; f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; g. Testowanie działania bramy 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS: a. Konfiguracja podstawowych parametrów b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań; c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego; d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; e. Testowanie działania ochrony IPS 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. a. Przypisanie adresu IP do zarządzania. b. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3 c. Definicja reguł filtrowania/blokowania d. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny. 8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej. 9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia. 10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN.

		11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC 12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności: a. kontrola dostępu - zapora ogniowa klasy Stateful Inspection b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS] d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) f. kontrola pasma oraz ruchu [QoS, Traffic shaping] g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P h. Ochrona przed wyciekiem poufnej informacji (DLP) i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL) j. Inspekcja ruchu SSL k. Ochrony przez atakami na stacje klienckie l. Kontrola pasma 13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi (np.: RCIM). 14. Konfiguracja logowania i raportowania.
6.	**Serwery pod wirtualizację**	Zamawiający wymaga instalacji i konfiguracji dostarczonych serwerów celem stworzenia bazy sprzętowej dla klastra niezawodnościowego i wydajnościowego stworzonego na bazie dostarczonych serwerów i oprogramowania do wirtualizacji.
7.	**Serwer backupu – rekonfiguracja.**	W ramach projektu przewiduje się wykorzystanie istniejącego serwera na miejsce przechowywanie backupu. Na serwerze należy zainstalować oprogramowanie do wirtualizacji – zarządzane z jednego centralnego miejsca, tego samego jak dla serwerów wirtualizacyjnych. System musi zostać podłączony do macierzy produkcyjnej, musie posiadać lokalne repozytoria danych na przestrzeni dyskowej, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na połowie zasobu dyskowego. Natomiast druga część zasobu musi zostać wykorzystana do wykonywania replikacji on-line maszyn wirtualnych na lokalna platformę wirtualizacyjną – na serwerze backupu. Takie podejście ma gwarantować zabezpieczenie kluczowych węzłów sieciowych (serwerów wirtualnych) na dwa sposoby tj. plik off-line maszyny wirtualnej oraz kopia on-line replikowania asynchronicznie według harmonogramu. Wykonywanie backupu musi być powiązane z procedurą sprawdzania poprawności jego wykonania oraz automatycznym raportowaniem do jednostki administracyjnej. Mechanizm podłączenia 1. Konfiguracja i podłączenie serwera backupu do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów

		wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 2. Konfiguracja i podłączenie serwera backupu do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 3. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.
8.	**Macierz dyskowa**	Macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych" – wykorzystywanych przez oprogramowanie dziedzinowe. Musi zostać podłączona do środowiska wirtualizacyjnego (klaster serwerów). Ilość i wielkość udziałów dyskowych udostępnionych dla serwerów np.: wirtualizacyjnych zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej.
9.	**Migracja danych**	Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów. Dane (systemy dziedzinowe) musza zostać przeniesione na nowe zasoby serwerowo-macierzowe. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych.
10.	**Serwer SMTP**	Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux. Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z: • Urządzeń sieciowych • Serwerów • Macierzy dyskowej • Systemu zarządzania kopiami zapasowymi • Systemu wirtualizacji serwerów • Aplikacji Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email.
11.	**Instalacja i konfiguracja serwera kopii zapasowych konfiguracji urządzeń sieciowych.**	1. Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.; przełączników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy. 2. Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego). 3. Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie.

		4. Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.
12.	**Uruchomienie środowiska wirtualizacyjnego.**	Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie: 1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta. 2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 3. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 4. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach. 5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów. 6. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 7. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 9. Przygotowanie koncepcji wirtualizacji fizycznych maszyn. 10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym. 11. Konfiguracja klastra wysokiej dostępności: a. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika. b. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn. c. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera. 12. Weryfikacja działania klastra wysokiej dostępności. 13. Migracja istniejącej infrastruktury do środowiska wirtualnego. 14. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową 15. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
13.	**System backupu**	1. Instalacja oprogramowania zarządzającego wykonywaniem kopii

		zapasowych. 2. Aktywacja oraz instalacja niezbędnych licencji. 3. Konfiguracja stacji zarządzającej. 4. Dołączenie klientów do system backupu. 5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania: a. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące; b. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy; c. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu; d. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową; e. musi istnieć możliwość odtworzenia: i. całej wirtualnej maszyny; ii. dysku wirtualnej maszyny; iii. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa); 6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej: a. Nazwę zadania backupu b. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/ c. Długość trwania zadania backupu d. Ilość zapisanych na taśmie danych 7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach: a. Błąd urządzenia b. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi c. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi d. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi e. Zdarzenia dotyczące licencji f. Zapełnienia mail-slotu 8. Uruchomienie testowych zadań backupu 9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email 10. Uruchomienie testowych zadań odtworzenia danych 11. Miejscem przechowywania kopii zapasowych jest: a. serwer backupu. b. na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu.
14.	**Usługa katalogowa.**	**Instalacja usługi katalogowej wraz z dodatkowymi komponentami w taki sposób, aby spełnione były poniższe wymagania celem świadczenia e-usług publicznych:**
14.1.	**Zaplanowanie liczby serwerów na potrzeby**	Taka liczba serwerów, aby w przypadku awarii pojedynczego serwera był zapewniony ciągły dostęp do usługi katalogowej, a w szczególności

	usługi katalogowej oraz serwerów plików	mechanizmy uwierzytelniania oraz rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na dostarczonym środowisku wirtualizacyjnym.
14.2.	**Wersja systemu operacyjnego serwerów**	Zastosowany system operacyjny musi zapewniać, co najmniej: a) możliwość uruchomienia usługi katalogowej w trybie usługi b) możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń c) możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem (w tym przynależność do grup zabezpieczeń) d) możliwość zarządzania usługą katalogową poprzez interfejs graficzny oraz CLI e) możliwość zainstalowania lokalnego Centrum Certyfikacji zapewniającego wydawanie niekwalifikowanych certyfikatów X.509 umożliwiających uwierzytelnianie na stacjach roboczych i serwerach z wykorzystaniem kart kryptograficznych, szyfrowanie danych
14.3.	**Instalacja systemu operacyjnego serwerów**	Instalacja systemu operacyjnego serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.
14.4.	**Uruchomienie usługi katalogowej oraz niezbędnych komponentów, migracja danych do/z obecnej usługi katalogowej**	Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem. Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego. Zamawiający wymaga skonfigurowania delegacji uprawnień do zadanych jednostek organizacyjnych dla administratorów niższego poziomu. Administratorzy niższego poziomu powinni mieć uprawnienia do: a) Resetowania haseł użytkowników b) Odblokowywania kont użytkowników c) Zmiany atrybutów „Display Name” oraz „Last name” Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi: a) Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości b) Śledzenie zmian dotyczących tworzenia, usuwania obiektów Zamawiający wymaga skonfigurowania dwóch stacji zarządzających. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).

14.5.	**Konfiguracja polityki haseł oraz polityki blokowania kont**	Konfiguracja globalnej polityki haseł dla domeny: a) Hasło musi zawierać minimum 8 znaków b) Maksymalny czas ważności hasła: do ustalenia z Zamawiającym c) Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym d) Hasło musi spełniać zasady złożoności Konfiguracja polityki haseł dla kadry zarządzającej: a) Hasło musi zawierać minimum 10 znaków b) Maksymalny czas ważności hasła: 30 dni c) Minimalny czas, po którym możliwa jest zmiana hasła: 240 dni d) Hasło musi spełniać zasady złożoności Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach. Szczegółowe dane zostaną przekazane na etapie konfiguracji.
14.6.	**Stworzenie skryptów służących do tworzenia struktury usługi katalogowej**	Po oddaniu wdrożonego systemu do eksploatacji konieczne będzie tworzenie nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych. Zamawiający oczekuje stworzenia przez Wykonawcę skryptów ułatwiających te zadania. **Założenia skryptu tworzącego nowe jednostki organizacyjne oraz grupy:** 1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie, co najmniej: a) ścieżki i nazwy pliku wejściowego b) ścieżki i nazwy pliku logującego c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu) d) nazwy FQDN domeny e) nazwy NetBIOS domeny f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty g) ścieżek do udziałów dyskowych SHARE1 oraz SHARE2 2. Skrypt ma pobierać z pliku wejściowego listę jednostek organizacyjnych 3. Skrypt tworzy nowe jednostki organizacyjne w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu 4. Skrypt tworzy nowe grupy zabezpieczeń o nazwie G_Nazwa_Jednoski_Organizacyjnej 5. Skrypt tworzy foldery: a) \\DOMENA\Public\SHARE1 b) \\DOMENA\Public\SHARE2 Foldery muszą posiadać tak ustawione parametry zabezpieczeń, aby użytkownicy nie mogli samodzielnie tworzyć nowych katalogów ani plików w lokalizacjach \\DOMENA\SHARE1 oraz \\DOMENA\SHARE2. 6. Skrypt tworzy podkatalogi: \\DOMENA\Public\SHARE1\Nazwa_Jednostki_Organizacyjnej oraz \\DOMENA\Public\SHARE2\Nazwa_Jednostki_Organizacyjnej 7. Skrypt nadaje uprawnienia do utworzonych podkatalogów według założeń: a) \\DOMENA\Public\SHARE1\Nazwa_Jednostki_Organizacyjnej: i. Administratorzy Domeny – Pełna kontrola

ii. Grupa G_Nazwa_Jednostki_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa_Jednostki_Organizacyjnej
iii. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu
iv. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze

a) \\DOMENA\Public\Share2\Nazwa_Jednostki_Organizacyjnej:

v. Administratorzy Domeny – Pełna kontrola
vi. Grupa G_Nazwa_Jednostki_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa_Jednostki_Organizacyjnej
vii. Użytkownicy Uwierzytelnieni - Odczyt
viii. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu
ix. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze

8. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina)
9. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania

Założenia skryptu tworzącego nowe konta użytkowników:

1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie co najmniej:
   a) ścieżki i nazwy pliku wejściowego
   b) ścieżki i nazwy pliku logującego
   c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu)
   d) nazwy FQDN domeny
   e) nazwy NetBIOS domeny
   f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty
   g) ścieżki do udziału sieciowego HOME
   h) litery dysku katalogu domowego
2. Skrypt ma pobierać z pliku wejściowego listę kont użytkowników w formacie: NazwaUzytkownika;Imie;Nazwisko:Haslo;Dzial;NumerTelefonu
3. Skrypt tworzy nowe konta użytkowników w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu pobierając wszystkie niezbędne dane z pliku wejściowego
4. Nowo utworzone konta użytkowników muszą mieć jednorazowo ustawione hasła – użytkownik musi zmienić hasło podczas pierwszego logowania
5. Skrypt tworzy katalog \\DOMENA\HOME\NazwaUzytkownika
6. Skrypt nadaje uprawnienia do utworzonych katalogów użytkowników według założeń:

		a) Administratorzy Domeny – Pełna kontrola b) Użytkownik – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu NazwaUzytkownika c) Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu d) Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 10. Skrypt ma ustawić dla każdego konta użytkownika literę dysku domowego oraz poprawną ścieżkę sieciową 11. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 12. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania 13. Skrypt ma wygenerować dla każdego zakładanego konta osobny plik tekstowy zawierający między innymi: Nazwę użytkownika, Imię, Nazwisko, Hasło do pierwszego zalogowania. Tak utworzone pliki mogą zostać wydrukowane i przekazane użytkownikom. Powyżej opisane skrypty muszą posiadać w treści kodu stosowne komentarze opisujące działanie skryptów. Skrypty zostanę przekazane Zamawiającemu w wieczyste użytkowanie bez dodatkowych opłat wraz ze stosowną dokumentacją użytkownika oraz szczegółową instrukcja obsługi. Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów.
14.7.	**Skonfigurowanie mapowania zasobów sieciowych**	Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows. Mapowane mają być między innymi zasoby: \\DOMENA\Public\SHARE1 \\DOMENA\Public\SHARE2 Oraz określone przez Zamawiającego drukarki sieciowe. Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby: 1. Z wykorzystaniem skryptów logowania 2. Z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows Vista i nowszych (Wymagane jest także skonfigurowanie automatycznej instalacji niezbędnych składników na stacjach klienckich. Zamawiający nie dopuszcza instalacji wymaganych składników ręcznie).
14.8.	**Uruchomienie i skonfigurowanie serwera plików oraz wydruków**	Zamawiający wymaga uruchomienie oraz skonfigurowanie serwerów plików oraz serwerów wydruków tak, aby były spełnione poniższe założenia: Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest zapewnieniem ciągłości dostępu do krytycznych danych Wnioskodawcy w przypadku awarii jednego z serwera plików.

		Zastosowane mechanizmy replikacji systemu plików muszą zapewniać: • Replikację multi-master z rozwiązywaniem konfliktów • Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki. Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu. Na serwerach plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów. Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących. Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty" oraz „Pulpit" ze stacji roboczych na serwery plików. Funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego. Zamawiający wymaga stworzenie domyślnego, obowiązującego profilu wędrującego dla klienckich systemów operacyjnych. Domyślny profil ma uwzględniać opracowanie i wykonanie grafiki na pulpit komputera klienta. Grafika będzie akceptowana przez Zamawiającego. Zamawiający wymaga stworzenia i przypisania odpowiednich polityk globalnych dla wymuszenia stosowania obowiązkowych (niemodyfikowalnych) profili mobilnych. Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji. Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi: a) Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder b) Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder c) Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień. Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera.
14.9.	**Serwery uwierzytelniające**	1. Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych. 2. Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na

		dwóch niezależnych serwerach. 3. Instancja serwera może być uruchomiona na serwerach domenowych z zastrzeżeniem, że będzie ona kompatybilna z usługami uruchomionymi na tych serwerach i nie będzie wpływać negatywnie na ich pracę. 4. Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach. 5. Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie.
14.10.	**Dołączenie stacji roboczych do domeny**	Zamawiający wymaga dołączenia wszystkich stacji roboczych do domeny. W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mająca na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (miedzy innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na konto domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji).
14.11.	**Uruchomienie usług umożliwiającą instalację i zarządzanie aktualizacjami stacji roboczych Windows**	Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów Windows według założeń: 1. Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet 2. Administrator zatwierdza aktualizacje do instalacji 3. Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu Zamawiający wymaga skonfigurowania co najmniej następujących parametrów: 1. Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje 2. Kategorii aktualizacji 3. Grup komputerów (KOMPUTERY, SERWERY, KOMPUTERY-TEST, SERWERY-TEST) 4. Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów 5. Zasad automatycznego zatwierdzania nowych aktualizacji. 6. Mechanizmów raportowania (email)
14.12.	**Przygotowanie infrastruktury PKI**	Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 10. Wymagana przez Zamawiającego konfiguracja zawiera co najmniej: 1. Zaplanowanie i uruchomienie wewnętrznej struktury CA 2. Konfiguracja szablonów certyfikatów 3. Wydanie certyfikatów dla serwerów oraz stacji roboczych 4. Zastosowanie mechanizmów bezpieczeństwa poprzez możliwość backupu archiwizacji kluczy prywatnych wydawanych certyfikatów. 5. Wskazanie wszystkich możliwych dróg publikacji list CRL 6. Instalacji i konfiguracji stacji (komputer PC) do wydania kart – stacja do personalizacji.
15.	**Testowanie i modyfikacja**	1. Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego.

	parametrów infrastruktury sieciowej.	2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. 3. Testowanie mechanizmów replikacji danych. 4. Testowanie dostępu publicznego do zasobów. 5. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu 6. Testowanie autoryzowanego dostępu do wewnętrznych zasobów. 7. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach
16.	**Asysty stanowiskowe**	Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia. Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego. Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego.
17.	**Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.**	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą. **Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.** W tym czasie przedstawiciel Wykonawcy: • zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. • dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności: a) zastosowanej technologii serwerów b) zastosowanej technologii pamięci masowej c) wirtualizacji d) systemu backupu e) zastosowanych rozwiązań aplikacyjnych Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania.
18.	**Opracowanie dokumentacji powykonawczej**	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu. 1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów. 2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).

		3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały. 5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.
19.	**Opieka serwisowa**	Zamawiający wymaga świadczenia opieki serwisowej przez okres 12 miesięcy z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych.