ZAMAWIAJĄCY:

GMINA SKOŁYSZYN
38-242 Skołyszyn 12
tel. /fax 13 4491062-64
e-mail: przetargi@skolyszyn.pl; gmina@skolyszyn.pl
strona internetowa: https://bip.skolyszyn.pl

Nr postępowania: GPIR.271.1.19.2022

Załącznik nr 1

Szczegółowy opis przedmiotu zamówienia

GMINA SKOŁYSZYN
38-242 Skołyszyn 12
tel./fax 13 44 910 62 (63) (64)
NIP 685-16-51-203 REGON 370440382
BS O/ Skołyszyn
76 8627 1037 2003 5000 0459 0001

Zatwierdzam:

WÓJT
mgr Bogusław Kręcisz
/Kierownik Zamawiającego/

Lipiec 2022

Spis treści

1 Wymagania ogólne dla urządzeń i oprogramowania sieciowego. 3
2 Wymagania gwarancyjne 3
3 Miejsce instalacji sprzętu i oprogramowania/systemu. 3
4 Ubezpieczenie sprzętu 3
5 Zestawienie zakresu dostaw i usług 4
5.1 Serwer do wirtualizacji – szt. 2 – wymagania minialne. 6
5.2 Macierz dyskowa – szt.1 – wymagania minimalne 9
5.3 Rozbudowa istniejącego serwera - szt. 1 – wymagania minimalne 12
5.4 Przełącznik sieci LAN – szt.2 – wymagania minimalne 12
5.5 Stacje robocze – szt.1 – wymagania minimalne 14
5.6 Oprogramowanie bazodanowe -szt.1 – wymagania minimalne. 22
5.7 Oprogramowanie do wirtualizacji – szt.1 – wymagania minimalne 25
5.8 Oprogramowanie domenowe – szt.1 – wymagania minimalne 26
5.9 Przedłużenie wsparcia dla urządzenia firewall – szt.1 – wymagania minimalne 29
5.10 Klucze VPN – 3 szt. – wymagania minimalne 29
5.11 Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania 29
5.12 Diagnoza cyberbezpieczeństwa 43

1 Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

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

2 Wymagania gwarancyjne.

Sprzęt

1. o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. roczna gwarancja (chyba, że zapisy szczegółowe stanowią inaczej) 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;
2. 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;
3. 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;
4. 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;
5. wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń sieciowych i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

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

3 Miejsce instalacji sprzętu i oprogramowania/systemu.

a. Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części załącznika na 1, w budynkach urzędu w miejscach wskazanych przez Zamawiającego.

4 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:

- 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.

- Do szkód objętych ubezpieczeniem zalicza się m.in. szkody wynikłe w następstwie:
  - działania człowieka:
    - niewłaściwej obsługi sprzętu, tj. nieostrożności, zaniedbania, niewłaściwego użytkowania,
    - braku kwalifikacji, błędu operatora itp.;
    - świadomego i celowego zniszczenia przez osoby trzecie, pracowników i współpracowników ubezpieczającego (jednak z zastosowaniem klauzuli reprezentantów),
  - 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.
  - 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
  - wody, tj. zalania wodą z urządzeń wodno – kanalizacyjnych, powodzi, wylewu wód podziemnych, a także czynników atmosferycznych w postaci mrozu, śniegu, deszczu wilgoci, pary wodnej itp.
  - wiatru, gradu, lawiny, obsunięcia i zapadania się ziemi, huraganu, trzęsienia ziemi,
  - zbyt wysokiego lub zbyt niskiego napięcia albo całkowitego zaniku napięcia w sieci instalacji elektrycznej, szkód przepięciowych i pochodnych powstałych w związku z uderzeniem pioruna,
  - sprzęt elektroniczny ubezpieczony jest również w zakresie szkód spowodowanych przez upadek.
- Dodatkowe rozszerzenie dotyczące ochrony sprzętu nie podłączonego na stanowisku pracy lub podczas przerwy w eksploatacji.

5 Zestawienie zakresu dostaw i usług.

Lp.	Nazwa	Długość gwarancji (minimum) [m-ce]	Ilość	Jednostka miary	Uwagi
1.	Serwer do wirtualizacji	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, min. 128 GB RAM, 2xSSD 480, 2x zasilacz, karta 2 porty 10G, karta 2 porty SAS 12G.
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, 24 zatoki dyskowe; 4 dyski SSD SAS min. 960 GB, 6 dysków 4TB.
3.	Rozbudowa istniejącego serwera	12 (kryterium oceny)	1	Szt.	Rozbudowywany serwer Fujitsu PRIMERGY RX2520 M5 będzie miejscem instalacji oprogramowania do backupu. Będzie odpowiadał za

					nadzór nad procesami backupu i archiwizacji danych oraz będzie dla nich repozytorium – miejscem ich składowania. Będzie to kolejny poziom bezpieczeństwa danych. Parametry: rozbudowa RAM o 64 GB (do 128 GB), karta 2 portowa 10G do podłączenia do sieci LAN.
4.	Przełącznik sieci LAN	12 (kryterium oceny)	2	Szt.	Pozycja uwzględnia zakup 2 szt. przełączników sieci LAN – 48 portowych 10/100/1000 Mbps z 4 portami uplink. Przełączniki będą stanowiły punkt podłączenia do sieci LAN istniejących komputerów w Urzędzie wraz dołączeniem się do rdzenia sieci z wykorzystaniem połączeń uplink 10G.
5.	Stacje robocze	12 (kryterium oceny)	11	Szt.	Pozycja dotyczy komputerów z oprogramowaniem do pracy biurowej. Typ AIO; 24 cale, 8 Gb RAM, 256 SSD, system operacyjny, oprogramowanie biurowe, gwarancja on-site NBD.
6.	Oprogramowanie bazodanowe	Nd.	1	Szt.	Pozycja uwzględnia koszt zakupu oprogramowania bazodanowego pozwalającego na uruchomienie centralnej bazy danych dla gromadzonych danych wykorzystywanych systemów informatycznych. Dodatkowo pozwoli na pobieranie danych do świadczonych e-usług publicznych dla mieszkańców oraz zapewni zdalną pracę pracowników urzędu. W kalkulacji uwzględniono licencję do pracy nas środowisku wirtualnym oraz zapewniającą dostęp zdalny. Licencja wieczysta na dana wersję produktu.
7.	Oprogramowanie do wirtualizacji	12 (kryterium oceny)	1	Szt.	Koszt zakupu dotyczy oprogramowania do wirtualizacji niezbędnego do stworzenia dedykowanego klastra niezawodnościowego na 2 fizycznych serwerach. Oprogramowanie konieczne do zapewnienia warunków pracy zdalnej i świadczenia e-usług publicznych przez gminę. Licencja wieczysta na wersję produktu.
8.	Oprogramowanie domenowe	Nd.	1	Szt.	Kalkulacja pozycji uwzględnia koszty 2 licencji systemu operacyjnego niezbędnego do funkcjonowania serwerów wirtualizacji oraz koszty licencji dostępowych (CAL) dla użytkowników (60 licencji). Zakup jest niezbędny do zapewnienia dostępu i funkcjonowania całej planowanej

					infrastruktury oraz utworzenia usługi katalogowej.
9.	Przedłużenie wsparcia dla urządzenia firewall	12 (kryterium oceny)	1	Szt.	Pozycja dotyczy zakupu wsparcia dla posiadanego przez Gminę sprzętu firewall zbudowanego w oparciu o urządzenie firmy Fortinet model FG-60E. Wykupione wsparcie pozwoli na zapewnieni dostępu do najnowszych wersji oprogramowani co zdecydowanie wpłynie na bezpieczeństwo pracy jak i świadczonych usług.
10.	Klucze VPN	Nd.	3	Szt.	Pozycja dotyczy zakupu kluczy dostępowych do posiadanego firewall'a poprzez zestawienia bezpiecznego kanału transmisji danych na publicznej sieci Internet - VPN. Uwierzytelnieni dwuskładnikowe. Zakup zwiększy poziom bezpieczeństwa dostępu do danych.
11.	Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania	12	1	Szt.	Usługi obejmować będą: a) Instalację i konfiguracje zakupionych urządzeń i oprogramowania. b) Migrację danych ze starych maszyn nowe środowisko wirtualizacyjne. c) Opracowanie polityk bezpieczeństwa sieci, przepływu danych. d) Instruktaż dla służb informatycznych. e) Wsparcie techniczne, nadzór autorski 12 miesięcy.
12.	Diagnoza cyberbezpieczeństwa	12	1	Szt.	Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina",

5.1 Serwer do wirtualizacji – szt. 2 – wymagania minimalne.

Lp.	Parametr lub warunek	Minimalne wymagania
1.	Obudowa	-Typu Rack, wysokość max. 2U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack. Możliwość montażu ramienia porządkującego przewody.
2.	Płyta główna	-Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów 18-rdzeniowych; -Sumarycznie minimum 6 złącz PCI Express, w tym minimum 3 złącza o prędkości minimum PCI Express x16 generacji 3; -Aktywne wszystkie złącza PCI-e. -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; -Zainstalowany moduł TPM 2.0 kompatybilny z systemem operacyjnym Windows Server 2022;
3.	Procesory	- Zainstalowane dwa procesory 8-rdzeniowe w architekturze x86 taktowane podstawowym zegarem o częstotliwości min. 3,2 GHz, osiągające wynik w testach

		wydajności SPECrate2017_int_base min. 121 pkt. przy konfiguracji z dwoma procesorami dla dowolnej platformy dwuprocesorowej producenta serwera, który jest oferowany w postępowaniu przez oferenta. Wymagane jest aby do oferty był załączony PDF ze strony spec.org. Nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych;
4.	Pamięć RAM	-Zainstalowane 128 GB pamięci RAM DDR4 typu Registered, 2933Mhz w kościach o pojemności 32 GB; -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC; -12 gniazd pamięci RAM na płycie głównej, obsługa minimum 768 GB pamięci RAM;
5.	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 3.0 RAID 0,1,5,10,50;
6.	Dyski twarde	-Zainstalowane min. 2 dyski SSD o pojemności 480 GB każdy, DWPD min.0,9, dyski Hotplug; -Minimum 4 wnęki dla dysków twardych Hotplug 3,5";
7.	Inne napędy zintegrowane	-Możliwość montażu napędu optycznego typu DVD-RW;
8.	Kontrolery LAN	-Wbudowana w płytę główną karta 2 x 1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express;
9.	Kontrolery I/O	-Zainstalowana karta SAS HBA wyposażona w dwa zewnętrze porty SFF 8644; -Wraz z serwerem należy dostarczyć min. 2 szt. kabli SAS (8644-8644) o długości min. 1m każdy;
10.	Porty	-zintegrowana karta graficzna ze złączem VGA; -7x USB 3.0, w tym minimum 2 na panelu przednim, minimum 1 wewnętrzne;
11.	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy maksymalnej 800W każdy; -Redundantne wentylatory; -Dwa kable zasilające C13-C14 o długości min. 4m każdy;
12.	Zarządzanie	-Wbudowane diody informacyjne informujące o stanie serwera; -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: 1. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; 2. 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; 3. Dostęp poprzez przeglądarkę Web; 4. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; 5. Zarządzanie alarmami (zdarzenia poprzez SNMP); 6. Możliwość przejęcia konsoli tekstowej; 7. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); 8. 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.); 9. Zainstalowana, dedykowana dla potrzeb karty zarządzającej pamięć flash o pojemności minimum 16 GB; 10. Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); 11. Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; 12. Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; 13. 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; 14. 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); 15. 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; 16. 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	1. Windows Server 2022, Windows Server 2019, Windows Server 2016, Suse, RHEL, Vmware 6.7 U3, 7.0 U1;
14.	Gwarancja	- gwarancja producenta serwera w trybie onsite z czasem reakcji w miejscu instalacji sprzętu najpóźniej w następnym dniu roboczym od zgłoszenia usterki; -Dostępność części zamiennych przez 5 lat od momentu zakupu serwera; -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; - Zgłoszenia serwisowe w języku polskim na dedykowany nr infolinii serwisowej producenta serwera; - W ofercie należy zamieścić stronę www producenta serwera (link), pod którą Zamawiający odnajdzie: nr tel. zgłoszeń serwisowych, adres email zgłoszeń serwisowych, formularz online zgłoszeń serwisowych producenta serwera. Nie dopuszcza się stron www podmiotów trzecich oraz nr kontaktowych/email/formularzy podmiotów trzecich. -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera

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; -Ogólnopolska, telefoniczna, polskojęzyczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji.

5.2 Macierz dyskowa – szt.1 – wymagania minimalne.

Lp.	Nazwa podzespołu	Minimalne wymagania
1.	Obudowa, możliwości rozbudowy macierzy	1) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19" z zajętością maks 2U w tej szafie. 2) Obudowa pojedynczego modułu rozwiązania – półka dyskowa, moduł kontrolerów -musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy 3) Macierz musi posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/macierzy; 4) Macierz nie może zawierać elementów typu bateria/akumulator wymagających jakiegokolwiek reżimu obsługowego: wymiana, przełączanie, ładowanie (np. nie dopuszcza się podtrzymania bateryjnego cache kontrolerów itp.) ; 5) Rozbudowa o dodatkowe moduły dyskowe (półki dyskowe) dla obsługiwanych dysków musi odbywać się wyłącznie poprzez zakup takich modułów tj. bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy; 6) Moduły (półki dyskowe) dla rozbudowy o dodatkowe dyski i przestrzeń dyskową muszą zapewniać możliwość instalacji co najmniej 24 dysków twardych 2,5" w półce o zajętości instalacyjnej nie większej niż 2U w szafach przemysłowych standardu 19"; 7) Macierz musi umożliwiać obsługę i rozbudowę do co najmniej 96 dysków twardych w jednym urządzeniu (zarządzane przez parę kontrolerów) 8) Połączenia pomiędzy półkami dyskowymi muszą zapewniać brak pojedynczego punktu awarii;
2.	Pojemność	1) System musi umożliwiać instalację dysków wykonanych w technologii hot-plug i wyposażonych w podwójny interfejs SAS, 2) Zainstalowane 4 szt. dysków SSD-SAS 12G o pojemności 960GB 3) Zainstalowane 6 szt. dysków NL-SAS 12G o pojemności 6TB
3.	Kontrolery	1) System musi obsługiwać 2 kontrolery pracujące w układzie nadmiarowym typu active-active i bez konieczności stosowania zewnętrznych połączeń kablowych pomiędzy nimi, z minimum 8GB pamięci podręcznej Cache w każdym kontrolerze, wymaga się dostarczenia minimum 2 kontrolerów;

		2) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik; 3) Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia. 4) Macierz musi pozwalać na wymianę kontrolera RAID bez utraty danych zapisanych na dyskach nawet w przypadku konfiguracji z jednym kontrolerem RAID; 5) W układzie z zainstalowanymi dwoma kontrolerami RAID zawartości pamięci podręcznej obydwu kontrolerów musi być identyczna tzw. cache mirror. 6) Każdy z kontrolerów RAID musi posiadać dedykowane min. 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością 1 Gb/s - dla zdalnej i lokalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy
4.	Interfejsy	1) Oferowana macierz musi być dostarczona w konfiguracji z minimum 2 portami SAS 12G na każdy kontroler macierzy, do podłączenia serwerów; 2) Dołączone 4 szt. przewodów SAS do podłączenia oferowanych serwerów;
5.	Poziomy RAID	Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1,1+0, 5, 5+0, 6
6.	Wspierane dyski	Oferowany model macierzy musi wspierać dyski: 1) dyski SAS wykonane w technologii hot-plug o pojemnościach o prędkościach obrotowych 10000 obrotów na minutę, 2) dyski NL-SAS (NearLine SAS) wykonane w technologii hot-plug o prędkości obrotowej min 7200 obrotów na minutę, 3) dyski SSD SAS wykonane w technologii hot-plug; 3) interfejsy obsługiwanych dysków muszą być wyposażone w minimum 2 porty pracujące w reżimie full-duplex (jednoczesna transmisję danych przez dwa porty) 4) Macierz musi wspierać mieszaną konfigurację dysków SSD, SAS i NearLine SAS w obrębie pojedynczego modułu obudowy 5) Macierz musi wspierać mechanizm automatycznej przedawaryjnej migracji zapisów i składowanych danych na dysk zapasowy. 6) Macierz musi wspierać technologię energooszczędne typu Drive Spin Down lub wyłączanie dysków nieaktywnych w trybie ręcznym i automatycznym z wykorzystaniem mechanizmu typu 'time scheduler' czyli w zadanym i/lub powtarzalnym oknie czasowym. 7) Macierz musi umożliwiać definiowanie i obsługę dysków zapasowych tzw. hot-spare w trybach: - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID - hot-spare dla zabezpieczania dowolnej grypy dyskowej RAID. 8) Macierz musi pozwalać na skonfigurowanie dowolnego dysku hot-plug dostarczonego w rozwiązaniu do roli dysku zapasowego jak w pkt.7 9) 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. BackLessCopy)
7.	Opcje software'owe	1) Macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na minimum 1024 kopie migawkowych. 2) Macierz musi wspierać Microsoft Volume ShadowCopy Services (VSS) 3) Macierz musi umożliwiać zdefiniowanie min. 1024 woluminów (LUN) 4) Macierz musi umożliwiać podłączenie logiczne z serwerami i stacjami poprzez minimum 4 ścieżki; 5) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID bez konieczności wyłączania macierzy lub bez konieczności wyłączania ścieżek dla podłączonych stacji/serwerów;

		6) Macierz musi umożliwiać rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD. 7) Oferowany model macierzy musi obsługiwać mechanizmy Thin Provisioning (przy zainstalowanych 2 kontrolerach) czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy – wymagana jest obsługa minimum 64 pól ThinProvisioning w rozwiązaniu. 8) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacji: - zmiana rozmiaru woluminu, - zmiana poziomu RAID, - zmiana technologii dysków dla danej grupy RAID, - dodawanie nowych dysków do istniejącej grupy dyskowej, 9) Macierz musi posiadać wsparcie dla systemów operacyjnych: MS Windows Server, SuSE Linux, RedHat Linux, Oracle Linux, Oracle VM, HP-UX, IBM AIX, SUN Solaris, Vmware, Citrix XEN Server 10) Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) 11) Macierz musi obsługiwać woluminy logiczne o maksymalnej pojemności minimum 128 TB. 12) Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji 13) Wraz z macierzą należy zapewnić wsparcie dla mechanizmów Off-loaded Data Transfer i Space Reclamation w środowiskach MS Windows 14) Wraz z macierzą należy zapewnić subskrypcję na bezpłatną aktualizację (możliwość bezpłatnego pobrania ze stron internetowych producenta) oprogramowania wewnętrznego macierzy w całym okresie obowiązywania gwarancji
8.	Konfiguracja, zarządzanie	1) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. 2) 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. Całe rozwiązanie musi być objęte gwarancją producenta z czasem przyjazdu inżyniera serwisu producenta na miejsce użytkowania najpóźniej w następnym dniu roboczym od zgłoszenia usterki do organizacji serwisowej producenta macierzy. 2. Serwis gwarancyjny musi obejmować dostęp do bezpłatnych poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia. 3. Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat. 4. System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. 5. Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych

		6. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia

5.3 Rozbudowa istniejącego serwera - szt. 1 – wymagania minimalne

Rozbudowa posiadanego serwerów PRIMERGY RX2520 M5: VFY:R2525SC190IN

- 2 szt. kości pamięci FUJITSU 32GB (1x32GB) 2Rx4 DDR4-2933 R ECC
- 1 szt. karta sieciowa 2x SFP+ PCI Express 10Gb do serwera

Dostarczone karty sieciowe muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą przejąć reżim serwisowy serwerów w których zostaną zainstalowane

5.4 Przełącznik sieci LAN – szt.2 – wymagania minimalne

Przełącznik wielowarstwowy L2/L3, zarządzany

Typ i liczba portów:
48 portów 10/100/1000BaseT RJ-45, 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 zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

Parametry wydajnościowe:
- Przepustowość przełącznika (switching bandwidth) 170 Gb/s
- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów 130 Mpps
- Pamięć DRAM – 512 MB
- Pamięć flash – 256 MB
- Procesor wbudowany 800 MHz
- Wielkość bufora pakietów – 1,5 MB
- 255 grup IGMP
- 4 grupy połączeń zagregowanych typu „port channel" LACP
- 8 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP
- 512 wpisów w listach kontroli dostępu ACL
- 8 kolejek sprzętowych

Obsługa:
- 255 aktywnych sieci VLAN
- 8 000 adresów MAC
- 32 statyczne trasy IPv4
- 16 interfejsów L3

Obsługa ramek Ethernet Jumbo 9 000 B

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

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
- 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 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 802.3af, 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

5.5 Stacje robocze – szt.11 – 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: • pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, • filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, • tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • automatyczne grupowanie poczty o tym samym tytule, • tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, • oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, • mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, • zarządzanie kalendarzem, • udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, • przeglądanie kalendarza innych użytkowników, • zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, • zarządzanie listą zadań, • zlecanie zadań innym użytkownikom, • zarządzanie listą kontaktów, p) udostępnianie listy kontaktów innym użytkownikom, • przeglądanie listy kontaktów innych użytkowników, • 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: 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, 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:

		o Na dedykowaną infolinie producenta komputera oraz na dedykowany adres email. o Poprzez formularz zgłoszeniowy online dostępny na stronie producenta komputera

5.6 Oprogramowanie bazodanowe -szt.1 – wymagania minimalne.

System bazodanowy (SBD) typ I licencjonowany na rdzenie procesora musi spełniać następujące wymagania poprzez wbudowane mechanizmy:

1. Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
5. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
6. SBD musi umożliwiać tworzenie klastrów niezawodnościowych.
7. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:
   - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
   - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
   - klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
8. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
9. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.
10. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.
11. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.
12. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń:
    - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),
    - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),

- para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).

13. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
14. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków" obiektu, „rodzica" itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.
15. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:
    - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
    - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
    - udostępniać język zapytań do struktur XML,
    - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
    - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.
16. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:
    - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
    - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
    - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
    - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).
17. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania.
18. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
19. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
20. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.
21. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.

22. System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:
    - mechanizm debuggowania tworzonego rozwiązania,
    - mechanizm stawiania „pułapek" (breakpoints),
    - mechanizm logowania do pliku wykonywanych przez transformację operacji,
    - możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),
    - możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)
    - mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),
    - mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),
    - mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
    - mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych.
23. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.
24. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).
25. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
26. Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
27. Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
28. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
29. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.

30. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać:
    - raporty parametryzowane,
    - cache raportów (generacja raportów bez dostępu do źródła danych),
    - cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),
    - współdzielenie predefiniowanych zapytań do źródeł danych,
    - wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
    - możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
    - możliwość wizualizacji wskaźników KPI,
    - możliwość wizualizacji danych w postaci obiektów sparkline.
31. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
32. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.
33. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.
34. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).
35. Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
36. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache'u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.
37. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.
38. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).

5.7 Oprogramowanie do wirtualizacji – szt.1 – wymagania minimalne

Licencja dla dostarczonych serwerów fizycznych posiadających 2 procesory z gwarancją utrzymania aktualnej wersji przez okres min. 1 roku,

- 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 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
- Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć
- i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 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 4 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 powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
- Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES, RHEL, Solaris, OS/2, NetWare, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu SCO OpenServer, SCO Unixware, Mac OS X.
- 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).

5.8 Oprogramowanie domenowe – szt.1 – wymagania minimalne

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Wymaga się aby oferowane licencje umożliwiały korzystanie 30 użytkownikom.
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 60 użytkowników (60 licencji dostępowych).

5.9 Przedłużenie wsparcia dla urządzenia firewall – szt.1 – wymagania minimalne

Pozycja dotyczy zakupu wsparcia dla posiadanego przez Gminę sprzętu firewall zbudowanego w oparciu o urządzenie firmy Fortinet model FG-60E. FC-10-0060E-950-02-DD - Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

5.10 Klucze VPN – 3 szt. – wymagania minimalne

Pozycja dotyczy zakupu kluczy dostępowych do posiadanego firewall'a (forinet – fortigate 60E) poprzez zestawienia bezpiecznego kanału transmisji danych na publicznej sieci Internet - VPN. Uwierzytelnieni dwuskładnikowe. Zakup zwiększy poziom bezpieczeństwa dostępu do danych. FortiTokenMobile (Electronic License) FTM-ELIC-5 Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5 users. Electronic license certificate.

5.11 Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania

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 • 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 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. 5. Instalacja i konfiguracja oprogramowania bazodanowego.
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 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. 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. 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.	Rekonfiguracja istniejącego urządzenia firewall/UTM w zakresie. 1. Przedłużenie wsparcia producenta zgodnie z ofertą Wykonawcy. 2. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 3. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta. 4. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 5. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu. 6. 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 7. 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 8. 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. 9. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej. 10. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia. 11. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN. 12. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC 13. 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 14. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi (np.: RCIM). 15. Konfiguracja logowania i raportowania. 16. Instalacja i konfiguracja w systemie firewall dostarczonych kluczy VPN.
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.	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.
8.	Serwer do tworzenia kopii.	W ramach projektu przewiduje się wykorzystanie istniejącego serwera na miejsce przechowywanie backupu. Serwer musi zostać rozbudowa zgodnie z wymaganiami OPZ.
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	Dołączenie serwera backupu do istniejącego oprogramowania backupu jako repozytorium danych – miejsce składowania i przechowywania danych 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, ay w przypadku awarii pojedynczego serwera był zapewniony ciągły dostęp do usługi katalogowej, a w szczególności mechanizmy uwierzytelniania oraz rozwiązywania nazw oraz serwera

	usługi katalogowej oraz serwerów plików	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 parametrów infrastruktury sieciowej.	1. Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego. 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) sieci LAN – przełączniki sieciowe b) firewall/UTM c) zastosowanej technologii serwerów d) zastosowanej technologii pamięci masowej e) wirtualizacji f) systemu backupu g) 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. Termin zakończenia zamówienia (wykonanie wszystkich prac instalacyjno - wdrożeniowych, oddanie systemu do eksploatacji) - **do 30.07.2023 r.**
19.	Opieka serwisowa	Zamawiający wymaga świadczenia opieki serwisowej przez okres 12 miesięcy z czasem reakcji na zaistniałe problemy wynoszącym 8 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych.

5.12 Diagnoza cyberbezpieczeństwa

Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina", opisanymi na stronie https://www.gov.pl/web/cppc/cyfrowa-gmina

Wykonawca musi wykonać usługę zgodnie zakresem oraz z formularzem stanowiącym załącznik do dokumentacji konkursowej. załączniku nr
Załącznik_nr_8_-_Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa

Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Termin wykonania diagnozy cyberbezpieczeństwa: **do 30.09.2022 r.**