Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Załącznik nr 3 do SWZ

Znak sprawy: OR.273.53.2022

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Tytuł

Nazwa postępowania: „Cyfryzacja i poprawa bezpieczeństwa informatycznego w ramach projektu „Cyfrowy Powiat"".

W ramach Projektu pn.:

„Polska Cyfrowa" na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji konkursu grantowego „Cyfrowy Powiat" o numerze POPC.05.01.00-00-0001/21-00

CPV:
30200000-1 Urządzenia komputerowe
48000000-8 Pakiety oprogramowania i systemy informatyczne

2. Zamawiający

	Powiat Zielonogórski
Adres:	ul. Podgórna 5 65-057 Zielona Góra
E-mail:	zamowienia@powiat-zielonogorski.pl
Telefon:	+ 48 68 452 7575

3. Termin wykonania Przedmiotu Zamówienia

Przedmiot Umowy musi być zrealizowany w terminie: 100 dni od dnia podpisania Umowy.

4. Przedmiot Zamówienia

Zakres prac Wykonawcy obejmuje dostawę infrastruktury sprzętowej wraz z oprogramowaniem oraz wszystkie inne prace instalacyjno-konfiguracyjne opisane przez Zamawiającego w SWZ oraz OPZ.

Realizacja Przedmiotu Zamówienia obejmuje przede wszystkim:

a) dostawę infrastruktury sprzętowej, oprogramowania specjalistycznego oraz rozbudowę zabezpieczeń logicznych opisanych w pkt.8 na warunkach określonych w SWZ oraz OPZ,
b) świadczenie usług gwarancyjnych.

Wykonawca jest zobowiązany dostarczyć Zamawiającemu wszelkie dokumenty gwarancyjne i licencyjne uprawniające do korzystania z infrastruktury sprzętowej oraz oprogramowania dostarczonego w ramach realizacji Przedmiotu Zamówienia.
Szczegółowy opis Przedmiotu Zamówienia został opisany w pkt.6, 7 oraz 8.

Uwaga:
Prace wdrożeniowe mogą być prowadzone w godz. 15.30 – 22.00 w dni robocze lub w innych godzinach ustalonych z Zamawiającym. Wykonywanie prac instalacyjnych oraz konfiguracyjnych przez Wykonawcę nie mogą zaburzyć ciągłości pracy Zamawiającego.

5. Środowisko Zamawiającego (stan obecny)

Stan obecny przedstawia wyłącznie komponenty dotyczące realizowanego Przedmiotu Zamówienia.

Uwaga:
Rozdział ten wyłącznie ma na celu pomóc Wykonawcy w doborze odpowiednich komponentów do rozbudowy istniejącej infrastruktury sprzętowej oraz adekwatnych licencji opisanych w pkt.8.

Komponent	Model	Producent
Zabezpieczenia logiczne typ I	FortiGate 100D nr seryjny FG100D3G17801190 Posiadana opcja: FortiGuard UTM Protection	Fortinet
Zabezpieczenia logiczne typ II	ESET Endpoint Protection Standard Liczba stanowisk: 150	ESET

6. Szczegółowy opis Przedmiotu Zamówienia (Zadania)

Zakres rzeczowy Przedmiotu Zamówienia obejmuje dostawę:

a) Stacji roboczej typ I (pkt.8.1),
b) Oprogramowania specjalistycznego typ I (pkt.8.2.),
c) Specjalistycznego urządzenia wielofunkcyjnego typ I (pkt.8.3),
d) Skanera typ I (pkt.8.4.),
e) Urządzenia wielofunkcyjnego typ I (pkt.8.5),
f) Rozbudowę zabezpieczeń technicznych typ I (pkt.8.6),
g) Rozbudowę zabezpieczeń technicznych typ II (pkt.8.7),
h) Oprogramowania specjalistycznego typ I (pkt.8.8.).
i) Stacji roboczej typ II (pkt.8.9.).

7. Wymagania ogólne

ID	Opis wymagania
7.1.	Dostarczane urządzenia muszą być fabrycznie nowe (nie wyprodukowane wcześniej niż 6 miesięcy przed datą dostawy) i pochodzić z oficjalnego kanału dystrybucyjnego producenta.
7.2.	Zamawiający zastrzega, by dostarczane urządzenia nie były używane przed ich dostawą i odbiorem. Uwaga: Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem.
7.3.	Opisane w pkt.8. wymagania stanowią zakres minimalnych oczekiwań Zamawiającego dla przedmiotu dostawy.
7.4.	W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne".
7.5.	W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 30 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne".
7.6.	Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w OPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.
7.7.	Wszystkie oferowane urządzenia elektryczne muszą spełnić wymogi niezbędne do oznaczenia produktu deklaracją CE.
7.8.	Całość dostarczonego sprzętu i oprogramowania musi zapewniać pełną kompatybilność, oraz jak najlepsze dopasowanie rozwiązań technicznych mających wpływ na pełną interoperacyjność gwarantującą bezkolizyjną integrację zamawianych komponentów na poziomie funkcjonalnym z istniejącą infrastrukturą Zamawiającego.
7.9.	Całość urządzeń musi być objęta gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależnie od statusu partnerskiego Wykonawcy przez okres **min. 12 miesięcy** od daty podpisania protokołu odbioru (chyba, że zapisy szczegółowe w pkt.8. stanowią inaczej).
7.10.	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.

8. Wytyczne dot. infrastruktury oraz oprogramowania

8.1. Stacja robocza typ I

ID	Opis wymagania
8.1.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Stacji roboczej typ I na warunkach określonych w SWZ.
8.1.2.	Stacja robocza typ I – komputer stacjonarny typu „All in One" (AIO) wykorzystywany do aplikacji biurowych i aplikacji dziedzinowych wykorzystywanych przez Zamawiającego.
8.1.3.	Procesor a) dedykowany do pracy w komputerach typu AIO, stosowany w układach jednoprocesorowych. osiągający min. 7800 pkt. w teście PassMark Single CPU zamieszczony na stronie: http://www.cpubenchmark.net/cpu_list.php w dniu zamieszczenia oferty SWZ na stronie Zamawiającego Uwaga: W przypadku jeżeli oferowany procesor nie jest zamieszczony na stronie http://www.cpubenchmark.net/cpu_list.php na Wykonawcy spoczywa obowiązek zamieszczenia wyników testów wydajności procesora i opublikowania parametrów wydajności procesora na powyższej stronie jednak nie później niż do dnia otwarcia złożonej oferty b) częstotliwość taktowania: min. 3GHz.
8.1.4.	Płyta główna: a) chipset zintegrowany, zaprojektowany do pracy w komputerach stacjonarnych dostosowany do zaoferowanego procesora, b) wyposażona w min. 2 sloty pamięci, c) zaprojektowana i wyprodukowana przez producenta komputera.
8.1.5.	Pamięć: a) zainstalowane: min. 8GB, b) typ: DDR4, c) min. 2666Mhz. d) liczba wolnych gniazd pamięci: min. 1 szt., e) max. wielkość pamięci: min. 64GB.
8.1.6.	Zainstalowane dyski twarde: a) min. 1 szt. dysków SSD min. 256GB, b) interfejs dysku SSD: PCI-Express.
8.1.7.	Obraz i dźwięk: a) przekątna ekranu: min. 21", b) typ matrycy: FHD IPS, c) powierzchnia matrycy: matowa, d) rozdzielczość: min. 1920 x min. 1080, e) wbudowana karta graficzna zintegrowana z płytą główną.
8.1.8.	Inne: a) obudowa: All-In-One b) porty USB: min. 2 x USB 2.0, c) porty USB: min. 2 x USB 3.0,

	d) min. 1x HDMI lub 1x DisplayPort, e) min. 1x RJ-45, f) kamera internetowa: tak, g) głośniki: tak.
8.1.9.	Akcesoria: a) Mysz, b) Klawiatura.
8.1.10.	Komunikacja: a) LAN 10/100/1000 Mbit/s, b) Bluetooth, c) Wi-Fi 802.11a/b/g/n/ac.
8.1.11.	Zainstalowany System operacyjny (SO) pochodzący z najnowszej linii produktowej Producenta SO. System operacyjny (SO) musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: a) system operacyjny nie wymaga aktywacji przez użytkownika, unikalny klucz produktu musi być umieszczony w BIOS/UEFI komputera. Upgrade Biosu (umieszczonego na stronie producenta płyty głównej) wykonanego przez Zamawiającego samodzielnie, nie może spowodować usunięcia klucza produktu zapisanego w BIOS/UEFI, b) interfejsy użytkownika dostępne w wielu językach do wyboru - w tym Polskim i Angielskim, c) możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji SO poprzez Internet, mechanizmem udostępnianym przez Producenta SO z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne, d) możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez Administratora Zamawiającego, e) wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, f) zintegrowana z SO konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6, g) graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, h) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), i) funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, j) możliwość zarządzania stacją roboczą poprzez polityki grupowe - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność SO lub aplikacji, k) możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania SO, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, l) zabezpieczony hasłem hierarchiczny dostęp do SO, konta i profile użytkowników zarządzane zdalnie, m) praca systemu w trybie ochrony kont użytkowników, n) zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna SO, o) system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,

	p) zintegrowany z SO moduł synchronizacji komputera z urządzeniami zewnętrznymi, q) wbudowany system pomocy w języku polskim, r) możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących), s) wsparcie dla IPSEC oparte na politykach - wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny, t) wsparcie dla uwierzytelniania na bazie Kerberos v.5, u) wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, v) wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec, w) wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk, x) wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach, y) wsparcie dla JScript i VBScript - możliwość uruchamiania interpretera poleceń, z) zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, aa) zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe, bb) przywracania obrazu plików systemowych do uprzednio zapisanej postaci. cc) zintegrowanie z usługą katalogową (Active Directory MS Windows, którą posiada zamawiający) dd) zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), WMI.
8.1.12.	Ilość: 14 szt.
8.1.13.	Gwarancja: min. 12 miesięcy gwarancji producenta w trybie on-site. Uwaga: Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.

8.2. Oprogramowanie specjalistyczne typ I

ID	Opis wymagania
8.2.1.	Zakres Przedmiotu zamówienia obejmuje dostawę licencji Oprogramowania specjalistycznego typ I na warunkach określonych w SWZ.
8.2.2.	Oprogramowanie specjalistyczne typ I – licencja Microsoft Office Standard 2021 CSP Lub oprogramowanie równoważne tj. pakiet biurowy spełniający wymagania opisane przez Zamawiającego w pkt.8.2 - poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji oraz musi zawierać co najmniej następujące komponenty: a) edytor tekstu, b) arkusz kalkulacyjny, c) narzędzia do przygotowywania i prowadzenia prezentacji, d) narzędzia do tworzenia drukowanych materiałów informacyjnych, e) program do zarządzania informacją przez użytkownika (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), f) narzędzia do tworzenia notatek, przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.

8.2.3.	Oprogramowanie specjalistyczne typ I musi umożliwiać: a) kopiowanie na wiele urządzeń przy wykorzystaniu jednego standardowego lub spersonizowanego obrazu przy użyciu jednego klucza licencyjnego b) swobodne przenoszenie między stacjami roboczymi (np. w przypadku wymiany sprzętu) c) musi zapewniać prawo do instalacji bezpłatnych aktualizacji udostępnionych przez producenta oprogramowania Uwaga: Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.
8.2.4.	Wszystkie komponenty oferowanego pakietu biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi.
8.2.5.	Dostępna pełna polska wersja językowa interfejsu użytkownika, systemu komunikatów i podręcznej kontekstowej pomocy technicznej.
8.2.6.	Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: doc, docx, xls, xlsx, ppt, pptx, pps, ppsx, w tym obsługa formatowania bez utraty parametrów i cech użytkowych (zachowane wszelkie formatowanie, umiejscowienie tekstów, liczb, obrazków, wykresów, odstępy między tymi obiektami i kolorów).
8.2.7.	Wykonywanie i edycja makr oraz kodu zapisanego w języku Visual Basic w plikach xls, xlsx oraz formuł w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013, MS Office 2016 oraz MS Office 2019 bez utraty danych oraz bez konieczności przerabiania dokumentów.
8.2.8.	Możliwość zapisywania wytworzonych dokumentów bezpośrednio w formacie PDF.
8.2.9.	Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory lub funkcjonalnie równoważną (użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się).
8.2.10.	Możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich elementów.
8.2.11.	Posiadać pełną kompatybilność z systemami operacyjnymi posiadanymi przez Zamawiającego: a) MS Windows 7 (32 i 64-bit), b) MS Windows 8 (32 i 64-bit), c) MS Windows 8.1 (32 i 64-bit), d) MS Windows 10 (32 i 64-bit). oraz sprzętem funkcjonującym u Zamawiającego.
8.2.12.	Tworzenie i edycja dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: a) posiada kompletny i publicznie dostępny opis formatu, b) posiada zdefiniowany układ informacji w postaci XML zgodnie z załącznikiem 2 do 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. z 2016 r., poz. 113), c) umożliwia wykorzystanie schematów XML,

	d) wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES, e) możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów oprogramowania, f) możliwość automatycznego odświeżania danych pochodzących z Internetu w wytworzonych dokumentach elektronicznych, np. w arkuszu kalkulacyjnym, g) możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów elektronicznych pozwalających na stwierdzenie, czy dany dokument lub arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony, h) możliwość automatycznego odzyskiwania dokumentów elektronicznych w wypadku nieoczekiwanego zamknięcia aplikacji, np. w wyniku wyłączenia zasilania komputera, i) prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: .DOC, .DOCX, .XLS, .XLSX, .XLSM, .PPT, .PPTX, .MDB, .ACCDB, w tym obsługa formatowania, makr, formuł i formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013, MS Office 2016 i MS Office 2019, bez utraty danych oraz bez konieczności reformatowania dokumentów, j) automatyczne wyróżnianie i aktywowanie hiperłączy w dokumentach podczas edycji i odczytu, k) oprogramowanie zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy), l) oprogramowanie umożliwia dostosowanie dokumentów i szablonów do potrzeb urzędu oraz udostępnianie narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców, m) dostępna jest pełna dokumentacja rozwiązania w języku polskim, n) wszystkie aplikacje w pakiecie oprogramowania biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi.
8.2.13.	Edytor tekstów musi umożliwiać: a) edycję i formatowanie tekstu w języku polskim, przy czym zapewniona jest obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalność autokorekty i słownika wyrazów bliskoznacznych, b) wstawianie i formatowanie tabel i obiektów graficznych, powiększanie obiektów na cały ekran, wstawianie obrazów i klipów wideo online, prowadnice wyrównania ułatwiające zestawianie wykresów, zdjęć i diagramów z tekstem, c) wstawianie tabel i wykresów z arkusza kalkulacyjnego, w tym tabel przestawnych, d) wykonywanie korespondencji seryjnej bazującej na danych adresowych, np. pochodzących z arkusza kalkulacyjnego, bazy danych, narzędzia do zarządzania informacją prywatną, e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel, rysunków, automatyczne tworzenie spisu treści, f) określenie układu stron (pionowa/pozioma), formatowanie nagłówków i stopek stron, wydruk dokumentów, g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, h) praca zespołowa, śledzenie i porównywanie zmian wprowadzonych w dokumencie przez użytkowników, prosta adiustacja zapewniająca przejrzysty widok dokumentu z zachowaniem oznaczeń miejsc wprowadzenia śledzonych zmian, komentarze z możliwością oznaczania ich jako gotowe i dodawania

	odpowiedzi, i) pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, Microsoft Word 2007, Microsoft Word 2010, Microsoft Word 2013, Microsoft Word 2016 i Microsoft Word 2019, z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, j) otwieranie plików PDF i edytowanie ich zawartości (w tym akapitów, list, tabel), k) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, l) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go jako środowiska udostępniającego formularze bazujące na schematach XML z centralnego repozytorium wzorów dokumentów elektronicznych (o którym mowa w art. 19b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r., poz. 1114), które po wypełnieniu umożliwiają zapisanie pliku XML, m) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 27 grudnia 2011 r. w sprawie wymagań technicznych dla dokumentów elektronicznych zawierających akty normatywne i inne akty prawne, dzienników urzędowych wydawanych w postaci elektronicznej oraz środków komunikacji elektronicznej i informatycznych nośników danych (Dz. U. z 2011 r., Nr 289, poz. 1699)
8.2.14.	Arkusz kalkulacyjny musi umożliwiać: a) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, zapis wielu arkuszy kalkulacyjnych w jednym pliku, formatowanie czasu, daty i wartości finansowych z polskim formatem, tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, automatyczne polecanie wykresu odpowiedniego do wprowadzonych danych, b) wyszukiwanie i zamianę danych, wykonywanie analiz danych przy użyciu formatowania warunkowego, nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, c) tworzenie raportów tabelarycznych, d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), możliwość osadzania fragmentów arkusza na stronie sieci Web, e) obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych; narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, f) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, automatyczne polecanie sposobów podsumowania danych, korzystanie z możliwości tworzenia układu tabeli przestawnej wykorzystującej jedną lub wiele tabel z wykorzystaniem tej samej listy pól, tworzenie relacji między tabelami, tworzenie osi czasu tabeli przestawnej w celu interaktywnego filtrowania dat, g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, h) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, Microsoft Excel 2007, Microsoft Excel 2010, Microsoft Excel 2013, Microsoft Excel 2016 i Microsoft Excel 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i

	makropoleceń, i) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
8.2.15.	Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a) przygotowywanie prezentacji multimedialnych, które będą prezentowane przy użyciu projektora multimedialnego, na monitorze lub tablecie, b) drukowanie w formacie umożliwiającym robienie notatek, c) zapisanie jako prezentacja tylko do odczytu, d) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, korzystanie z formatu panoramicznego i rozdzielczości HD, nagrywanie narracji i dołączanie jej do prezentacji, ułatwienia wyrównywania obiektów i stosowania jednakowych odstępów, e) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, f) możliwość tworzenia animacji obiektów i całych slajdów, g) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, h) pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, MS PowerPoint 2010, MS PowerPoint 2013 i MS PowerPoint 2016.
8.2.16.	Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: a) tworzenie i edycję drukowanych materiałów informacyjnych, podział treści na kolumny, umieszczanie elementów graficznych, b) tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów, c) płynne przesuwanie elementów po całej stronie publikacji, tworzenie tła z obrazów, stosowanie efektów do obrazów i tekstu (np. cienia, odbicia, poświaty, obrotów 3-W), d) wydruk publikacji, wykorzystanie mechanizmu korespondencji seryjnej, e) eksport publikacji do formatu PDF oraz TIFF, f) możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
8.2.17.	Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego MS Exchange 2010/2013/2016, b) przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, c) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, d) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, automatyczne grupowanie poczty o tym samym tytule, e) wspieranie funkcji asystenta podczas nieobecności, f) 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, g) zarządzanie kalendarzem, udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, przeglądanie kalendarza innych użytkowników, h) zapraszanie uczestników na spotkania, co po ich akceptacji powoduje

	automatyczne wprowadzenie spotkania w ich kalendarzach, i) zarządzanie listą zadań, zlecanie zadań innym użytkownikom, j) zarządzanie listą kontaktów, udostępnianie listy kontaktów innym użytkownikom, przeglądanie listy kontaktów innych użytkowników, możliwość przesyłania kontaktów innym użytkowników
8.2.18.	Ilość: 14 szt.

8.3. Specjalistyczne urządzenie wielofunkcyjne typ I

ID	Opis wymagania
8.3.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Specjalistycznego urządzenia wielofunkcyjnego typ I.
8.3.2.	Specjalistyczne urządzenie wielofunkcyjne typ I - kolorowe laserowe urządzenie wielofunkcyjne A3.
8.3.3.	Wymagane funkcje: a) drukowanie, b) kopiowanie, c) skanowanie, d) wysyłanie.
8.3.4.	Procesor: częstotliwości min. 1.8 GHz.
8.3.5.	Pamięć RAM: min. 5GB.
8.3.6.	Dysk twardy: SSD min. 250GB.
8.3.7.	Interfejsy: a) 1000Base-T/100Base-TX/10Base-T, b) bezprzewodowa sieć LAN (IEEE 802.11 b/g/n), c) USB 2.0, d) USB 3.0.
8.3.8.	Panel sterowania: a) dotykowy, b) kolorowy, c) min. 10-calowy.
8.3.9.	Obsługa: a) czujnik ruchu wykrywający zbliżającego się użytkownika i wybudzający urządzenie z trybu uśpienia.
8.3.10.	Prędkość drukowania: a) A4 mono: min. 40 str./min, b) A4 kolor: min. 40 str./min, c) A3 mono: min. 20 str./min, d) A3 kolor: min. 20 str./min.
8.3.11.	Czas nagrzewania: max. 4 sek.
8.3.12.	Rozdzielczość drukowania rzeczywista (nie interpelowana): min. 1200 x min. 1200 dpi
8.3.13.	Język opisu strony: a) PCL 6, b) oryginalny Adobe PostScript3 (nie emulacja).
8.3.14.	Dupleks: Automatyczny.
8.3.15.	Wydruk plików z pamięci USB: TAK, Obsługiwane formaty (zakres minimalny):

	a) PDF, b) JPEG, c) TIFF, d) EPS, e) XPS.
8.3.16.	Inne: a) obsługa wstrzymywania wydruków - możliwość zdefiniowania na urządzeniu polityki wstrzymywania wszystkich lub wybranych wydruków, b) możliwość zarządzania swoją kolejką wstrzymanych prac na pulpicie urządzenia, po identyfikacji użytkownika kodem PIN (opcjonalnie kartą), c) podgląd wstrzymanego dokumentu, zmiana opcji wykończeniowych, zwolnienie do druku lub wykasowanie pracy.
8.3.17.	Skaner: a) płaski, b) kolorowy jednoprzebiegowy, c) dwustronny podajnik oryginałów umożliwiający jednoczesne skanowanie dwustronnego dokumentu w jednym przejściu arkusza.
8.3.18.	Rozdzielczość skanowania: min. 600 x min. 600dpi.
8.3.19.	Pojemność jednoprzebiegowego podajnika dokumentów: min. 100 arkuszy o gramaturze min. 80 g/m2.
8.3.20.	Prędkość skanowania dwustronnego: a) mono: min. 250 obr./min przy 300x300dpi, b) w kolorze: min. 250 obr./min przy 300x300dpi.
8.3.21.	Format plików: a) TIFF, b) JPEG, c) PDF, d) PDF/A-1b, e) XPS.
8.3.22.	OCR: Tak Uwaga: Wymagany wbudowany moduł OCR bez limitu stron i licencji pozwalający skanować do formatów (zakres minimalny): a) Word, b) PowerPoint, c) PDF.
8.3.23.	Czas uzyskania pierwszej kopii: a) mono: max. 5s, b) kolor: max. 7s.
8.3.24.	Kopiowanie ciągłe: 1-999.
8.3.25.	Powiększanie dokumentów: od min. 25% - do max. 400%.
8.3.26.	Kopiowanie dwustronne: Tak (kopiowanie dwustronne oryginałów na dwustronne kopie).
8.3.27.	Kasety na papier: a) obsługujące koperty: min. 2 szt., b) obsługująca format papieru A5R-A3: min. 1 szt..
8.3.28.	Pojemność kaset na papier: każda na min. 500 arkuszy o gramaturze min. 80 g/m2.
8.3.29.	Obsługiwana gramatura papieru z podajnika bocznego: min. 55 g/m2 – max. 300 g/m2.
8.3.30.	Podajnik boczny:

	a) obsługujący gramaturę min. 55 g/m2 – max. 300 g/m2, b) obsługujący formaty: A5-A3, c) wydruk na papierze powlekanym.
8.3.31.	Pojemność tacy odbiorczej: a) min. 200 arkuszy o gramaturze min. 80 g/m2.
8.3.32.	Finiszer: a) możliwość rozbudowy o finiszer wewnętrzny zszywający posiadający funkcję zszywacza ekologicznego (bezzszywkowego) oraz funkcję zszywania na żądanie.
8.3.33.	Bezpieczeństwo: a) szyfrowanie dysku twardego, b) obsługa protokołu TLS 1.3.
8.3.34.	Oprogramowanie: a) oparte na chmurze (bez potrzeby instalacji lokalnego serwera), Umożliwiające: a) śledzenie i raportowanie kosztów, generowanych przez poszczególnych użytkowników, powstałych poprzez wykonanie określonych ilości kopii/wydruków/skanów. b) możliwość centralnego definiowania identyfikatorów użytkowników (numerów kart lub kodów PIN), c) możliwość przydzielania uprawnień do poszczególnych funkcji urządzeń, np. kolor czy skanowanie, d) możliwość rozbudowy o kolejne urządzenia tej samej marki, bez konieczności zakupu dodatkowych licencji.
8.3.35.	Ilość: 1 szt.
8.3.36.	Gwarancja: min. 12 m-cy.

8.4. Skaner typ I

ID	**Opis wymagania**
8.4.1	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Skanera typ I.
8.4.2	Skaner typ I - Skaner sieciowy z podajnikiem arkuszy.
8.4.3	Typ skanera: Skaner z podajnikiem.
8.4.4	Rozdzielczość: a) optyczna (automatyczny podajnik dokumentów): min. 600 dpi x min. 600 dpi, b) skanowania: min. 600 dpi x min. 600 dpi..
8.4.5	Rozmiar dokumentu (ADF): a) min.: 55 mm x 55 mm (poziomo x pionowo), b) max.: 210 mm x 6000 mm (poziomo x pionowo).
8.4.6	Formaty papieru a) A4 (21.0x29,7 cm), b) A5 (14,8x21,0 cm), c) A6 (10,5x14,8 cm), d) B4, B5, B6, e) Letter, f) Legal, g) Pocztówka, h) Wizytówki, i) Plastikowe karty,

	j) DL (koperta).
8.4.7	Głębia kolorów: a) Wejście (kolor/mono): min. 30 Bit / min. 10 Bit, b) Wyjście (kolor/mono): min. 24 Bit / min. 8 Bit.
8.4.8	Interfejsy: a) USB 2.0, b) Ethernet (1000 Base-T/ 100-Base TX/ 10-Base-T).
8.4.9	Układ optyczny: CIS (stykowy przetwornik obrazu).
8.4.10	Prędkość skanowania (A4): a) mono: min. 40 str./min., b) kolor: min. 40 str./min..
8.4.11	Inne: a) podajnik dokumentów (ADF): Tak, b) wyświetlacz LCD: Tak, c) Ultradźwiękowy czujnik: Tak.
8.4.12	Rodzaj automatycznego podajnika dokumentów: a) skanowanie dwustronne jednoprzebiegowe, b) skanowanie dwustronne (dupleks): Tak, c) ilość stron: min. 100.
8.4.13	Zaawansowana integracja dokumentu – skanowanie: a) do e-maila, b) na FTP, c) do katalogu web, d) do katalogu.
8.4.14	Funkcje kompresji pliku: a) TIFF (JPEG(7), b) CCITT G4, LZW), c) Kompresja PDF, d) Kompresja JPEG.
8.4.15	Wolumen skanowania: a) liczba stron dziennie: min. 4000.
8.4.16	Ilość: 3 szt.
8.4.17	Gwarancja: mn. 12 m-cy.

8.5. Urządzenie wielofunkcyjne typ I

ID	**Opis wymagania**
8.5.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Urządzenia wielofunkcyjnego typ I.
8.5.2.	Urządzenie wielofunkcyjne typ I - wielofunkcyjne kolorowe urządzenie laserowe.
8.5.3.	Wymagane funkcje: a) drukowanie, b) kopiowanie, c) skanowanie.
8.5.4.	Procesor: częstotliwości min. 1200 MHz.
8.5.5.	Pamięć RAM: min. 1GB.
8.5.6.	Interfejsy (zakres minimalny): a) 1000Base-T/100Base-TX/10Base-T, b) bezprzewodowa sieć LAN (IEEE 802.11 b/g/n),

	c) USB 2.0 Hi-Speed.
8.5.7.	Panel sterowania: a) dotykowy, b) kolorowy.
8.5.8.	Prędkość drukowania: a) A4 (mono/kolor): min. 30 str/min.
8.5.9.	Czas wydruku pierwszej strony: max. 7.5 sek.
8.5.10.	Rozdzielczość drukowania rzeczywista (nie interpelowana): min. 1200 x min. 1200 dpi.
8.5.11.	Języki obsługi drukarki: a) UFRII, b) PCL 5e1, PCL6, c) Adobe® PostScript3.
8.5.12.	Dupleks: Automatyczny.
8.5.13.	Wydruk plików z pamięci USB: TAK, Obsługiwane formaty (zakres minimalny): a) PDF, b) JPEG, c) TIFF.
8.5.14.	Automatyczny podajnik dokumentów: a) jednoprzebiegowy podajnik na min. 50 ark. (80g/m2).
8.5.15.	Skaner: a) płaski, b) kolorowy jednoprzebiegowy.
8.5.16.	Rozdzielczość skanowania: min. 600 x min. 600dpi.
8.5.17.	Format plików: a) TIFF, b) JPEG, c) PDF.
8.5.18.	OCR: a) wbudowany moduł OCR bez limitu stron i licencji pozwalający skanować do przeszukiwalnego PDF.
8.5.19.	Skanowanie do pamięci USB oraz smartfonów: tak.
8.5.20.	Kopiowanie ciągłe: 1-999.
8.5.21.	Powiększanie dokumentów: od min. 25% - do max. 400%.
8.5.22.	Kopiowanie dwustronne: Tak (kopiowanie dwustronne oryginałów na dwustronne kopie).
8.5.23.	Kasety na papier: a) 1 szt. kaseta na papier, b) obsługująca format papieru A4-A6. c) pojemność: min. 250 arkuszy o gramaturze 80 g/m2.
8.5.24.	Obsługiwana gramatura papieru z podajnika bocznego: min. 60 g/m2 – max. 200 g/m2.
8.5.25.	Podajnik boczny – rozmiary nośników: a) A4, A5, A5 (układ poziomy), A6, b) B5, Legal, Letter, c) pocztówki, karty indeksowe, d) koperty (COM10, DL, C5, Monarch).
8.5.26.	Pojemność tacy odbiorczej: a) min. 150 arkuszy o gramaturze min. 80 g/m2.
8.5.27.	Oprogramowanie: a) oparte na chmurze (bez potrzeby instalacji lokalnego serwera)

	Umożliwiające: a) śledzenie i raportowanie kosztów generowanych przez poszczególnych użytkowników, powstałych poprzez wykonanie określonych ilości kopii/wydruków/skanów. b) możliwość centralnego definiowania identyfikatorów użytkowników (numerów kart lub kodów PIN), c) możliwość przydzielania uprawnień do poszczególnych funkcji urządzeń, np. kolor czy skanowanie, d) możliwość rozbudowy o kolejne urządzenia tej samej marki, bez konieczności zakupu dodatkowych licencji.
8.5.28.	Ilość: 10 szt.
8.5.29.	Gwarancja: min. 12 m-cy.

8.6. Rozbudowa zabezpieczeń logicznych typ I

ID	Opis wymagania
8.6.1.	Zakres Przedmiotu zamówienia obejmuje Rozbudowę zabezpieczeń technicznych typ I.
8.6.2.	Przedmiotem zamówienia jest zakup/wymiana/trade up urządzeń posiadanych przez Zamawiającego: FortiGate 100D nr seryjny FG100D3G17801190 Posiadana opcja: FortiGuard UTM Protection do wersji **co najmniej FortiGate 100F** wraz z abonamentem i wsparciem technicznym na okres min. 12 miesięcy lub rozwiązanie równoważne opisane przez Zamawiającego w pkt.8.6. wraz z usługą wdrożenia (montaż, podłączenie, konfiguracja ustawień, polityk, obiektów, reguł – przeniesienie konfiguracji i ustawień z dotychczasowego urządzenia na nowe urządzenie). Zamawiający dopuszcza wymianę urządzeń FortiGate (TradeUp) - w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca musi przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004 r. Nr 229, poz. 2315, z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
8.6.3.	W przypadku zaoferowania rozwiązania równoważnego rozwiązanie to musi być w pełni kompatybilne z posiadanymi już przez Zamawiającego urządzeniami opisanymi w pkt.5. W przypadku dostarczenia rozwiązania innego producenta niż posiada Zamawiający,

	Wykonawca zapewni przeszkolenie personelu technicznego tj. Administratorzy – min. 2 osoby z dostarczonego rozwiązania w autoryzowanym ośrodku szkoleniowym na ternie kraju.
8.6.4.	Wymagania ogólne: a) system bezpieczeństwa musi realizować wszystkie opisane przez Zamawiającego w pkt.8.6 funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza, b) Zamawiający dopuszcza iż poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia Uwaga: W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. c) system realizujący funkcję Firewall musi zapewniać pracę w jednym z trzech trybów: i. routera z funkcją NAT, ii. transparentnym, iii. monitorowania na porcie SPAN. d) system musi umożliwiać budowę min. 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: i. routingu, ii. firewall'a, iii. IPSec VPN, iv. Antywirus, v. IPS, vi. Kontroli Aplikacji. e) system musi wspierać protokoły IPv4 oraz IPv6 w zakresie: i. Firewall, ii. ochrony w warstwie aplikacji. iii. protokołów routingu dynamicznego.
8.6.5.	Interfejsy: a) GE RJ45: min. 16 szt., b) GE SFP: min. 4 szt., c) współdzielone GE RJ45 / SFP: min. 4 szt. d) 10 GE SFP+: min. 2 szt., e) GE RJ45 WAN: min. 2 szt., f) Console Port: min. 1 szt., g) USB Uwaga: Gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
8.6.6.	Firewall musi umożliwiać konfigurację: a) min. 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
8.6.7.	Parametry wydajnościowe: a) przepustowość Firewall: i. pakiety UDP 1518 bajtów: min. 20 Gbps,

	ii. pakiety UDP 512 bajtów: min. 18 Gbps, iii. pakiety UDP 64 bajtów: min. 10 Gbps, b) wydajność szyfrowania IPSec VPN IPsec (512 bajtów): min. 11 Gbps Uwaga: Test wydajności VPN IPsec używa AES256-SHA256. c) opóźnienie Firewall (64 bajtowe pakiety UDP): max. 5 µs, d) obsługa: i. jednoczesne połączenia (sesje równoległe) (TCP): min. 1.4 mln., ii. nowe połączenia: min. 52.000, e) Tunele VPN IPsec: i. Gateway-to-Gateway: min. 2500, ii. Client-to-Gateway: min. 16000, f) przepustowość SSL-VPN: min. 1 Gbps, g) wydajność inspekcji SSL (IPS, HTTP) (ang. SSL Inspection Throughput): min. 1 Gbps. Uwaga: Wartości wydajności SSL Inspection mierzona z wykorzystaniem średniej sesji HTTPS dla różnych zestawów szyfrów. h) wydajność skanowania ruchu typu Enterprise Mix: i. IPS Throughput: min. 2.5 Gbps, ii. NGFW Throughput (z włączonymi funkcjami: IPS, Application Control, Antywirus): min. 1.6 Gbps, iii. Threat Protection Throughput (z włączonymi funkcjami: IPS, Application Control, Antywirus): min. 1 Gbps.
8.6.8.	Redundancja, monitoring i wykrywanie awarii: a) w przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive Uwaga: W obu trybach system firewall musi zapewniać funkcję synchronizacji sesji, b) monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. c) monitoring stanu realizowanych połączeń VPN, d) agregacja linków: i. statyczna ii. w oparciu o protokół LACP.
8.6.9.	Konfiguracje wysokiej dostępności (HA - High Availability): a) Aktywny/Aktywny, b) Aktywny/Pasywny, c) Clustering (Grupowanie).
8.6.10.	Funkcje systemu bezpieczeństwa (Zamawiający dopuszcza realizację funkcji w postaci osobnych, komercyjnych platform sprzętowych lub programowych): a) kontrola dostępu - zapora ogniowa klasy Stateful Inspection, b) kontrola Aplikacji, c) poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN, d) ochrona przed malware, e) ochrona przed atakami - Intrusion Prevention System. f) kontrola stron WWW, g) kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3,

	h) zarządzanie pasmem (QoS, Traffic shaping), i) mechanizmy ochrony przed wyciekiem poufnej informacji (DLP), j) dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych Uwaga: Min. 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site, k) inspekcja (min. IPS) ruchu szyfrowanego protokołem SSL/TLS, min. dla następujących typów ruchu: i. HTTP (w tym HTTP/2), ii. SMTP, iii. FTP, iv. POP3, d) funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system, e) wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
8.6.11.	Polityki, Firewall a) polityka Firewall uwzględnia: i. adresy IP, ii. użytkowników, iii. protokoły, iv. usługi sieciowe, v. aplikacje lub zbiory aplikacji, vi. reakcje zabezpieczeń, vii. rejestrowanie zdarzeń, b) translacja adresów NAT: źródłowego i docelowego, translację PAT oraz: i. translację jeden do jeden oraz jeden do wielu, ii. dedykowany ALG (Application Level Gateway) dla protokołu SIP, c) możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN, d) możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: i. kategorie URL, ii. adresy IP. e) filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe, f) możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna, g) element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. i. Amazon Web Services (AWS), ii. Microsoft Azure, iii. Cisco ACI, iv. Google Cloud Platform (GCP), v. OpenStack,

	vi. VMware NSX, vii. Kubernetes.
8.6.12.	Połączenia VPN: a) możliwość konfiguracji połączeń typu IPSec VPN: i. wsparcie dla IKE v1 oraz v2, ii. obsługa szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM), iii. obsługa protokołu Diffie-Hellman grup 19, 20, iv. wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, v. tworzenie połączeń typu Site-to-Site oraz Client-to-Site, vi. monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, vii. możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego, viii. wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat, ix. możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu, x. możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu, xi. obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth, xii. mechanizm „Split tunneling" dla połączeń Client-to-Site. b) możliwość konfiguracji połączeń typu SSL VPN: i. praca w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki (komunikacja działającą w oparciu o HTML 5.0), ii. praca w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. Uwaga: Producent rozwiązania musi posiadać w swojej ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn dostępne jako opcja – funkcjonalność nie należy uwzględniać w cenie oferty.
8.6.13.	Routing i obsługa łączy WAN, w tym przede wszystkim obsługa: a) routingu statycznego, b) Policy Based Routing (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). c) protokołów dynamicznego routingu w oparciu o protokoły: i. RIPv2 (w tym RIPng), ii. OSPF (w tym OSPFv3), iii. BGP, iv. PIM, d) możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu, e) ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu, f) BFD (Bidirectional Forwarding Detection), g) monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
8.6.14.	Funkcje SD-WAN:

	a) system musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN, b) wsparcie dla interfejsów fizyczne jak i wirtualnych (w tym VLAN, IPSec).
8.6.15.	Zarządzanie pasmem: a) system Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: i. maksymalnej i gwarantowanej ilości pasma, ii. oznaczanie DSCP, iii. wskazanie priorytetu ruchu. b) możliwość określania pasma dla poszczególnych aplikacji, c) możliwość definiowania pasma dla wybranych użytkowników niezależnie od ich adresu IP, d) możliwość zarządzania pasmem dla wybranych kategorii URL.
8.6.16.	Ochrona przed malware: a) silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021), b) silnik antywirusowy musi zapewniać skanowanie następujących protokołów: i. HTTP, ii. HTTPS, iii. FTP, iv. POP3, v. IMAP, vi. SMTP, CIFS. c) skanowanie archiwów, w tym co najmniej: i. Zip, ii. RAR. Uwaga: W przypadku archiwów zagnieżdżonych system musi możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości, d) blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów, e) system musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android), f) Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora, g) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze, h) usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików, i) możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta, j) możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
8.6.17.	Ochrona przed atakami: a) ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych, b) ochrona przed atakami na aplikacje pracujące na niestandardowych portach, c) baza sygnatur ataków musi zawierać min. 5000 wpisów i być aktualizowana

	automatycznie, zgodnie z harmonogramem definiowanym przez administratora, d) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur, e) wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. f) mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty), g) możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http, h) wykrywanie i blokowanie komunikacji C&C do sieci botnet, i) możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Uwaga: Mechanizmy ochrony IPS nie mogą działać globalnie.
8.6.18.	Kontrola aplikacji: a) funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP, b) baza Kontroli Aplikacji musi zawierać min. 2000 sygnatur i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora, c) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików, d) baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, e) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur, f) możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021), g) możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
8.6.19.	Kontrola WWW a) moduł kontroli WWW musi korzystać z bazy zawierającej min. 40 milionów adresów URL pogrupowanych w kategorie tematyczne, b) w ramach filtra WWW dostępne kategorie istotne z punktu widzenia bezpieczeństwa: i. malware (lub inne będące źródłem złośliwego oprogramowania), ii. phishing, iii. spam, iv. Dynamic DNS, v. proxy. c) filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard. d) administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL, e) filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwalać definiować strony z zastosowaniem wyrażeń regularnych (Regex), f) filtr WWW musi umożliwiać wykonanie akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej

	strony, g) zaimplementowana funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo, h) administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW, i) system musi umożliwiać określenie, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
8.6.20.	Uwierzytelnianie użytkowników w ramach sesji: a) system Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: i. haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, ii. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, iii. haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. b) możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego, c) możliwość budowy architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. d) uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
8.6.21.	Zarządzanie: a) elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania, b) komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów, c) możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. d) współpraca z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow, e) możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację, f) element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall, g) element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone, h) możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM), i) możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
8.6.22.	Logowanie: a) elementy systemu bezpieczeństwa muszą umożliwiać logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. b) w ramach logowania element systemu pełniący funkcję Firewall musi zapewniać przekazywanie danych o:

	i. zaakceptowanym ruchu, ii. blokowanym ruchu, iii. aktywności administratorów, iv. zużyciu zasobów, v. stanie pracy systemu, możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. c) logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa, d) możliwość włączenia logowania per reguła w polityce firewall, e) możliwość logowania do serwera SYSLOG, f) możliwość przesyłania SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
8.6.23.	Certyfikaty a) poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall
8.6.24.	Wykaz wymaganych czynności instalacyjnych: a) ustalenie projektu wdrożenia w uzgodnieniu z Zamawiającym, b) montaż urządzenia w środowisku Zamawiającego, c) podłączenie urządzenia, d) odtworzenie obecnej konfiguracji i ustawień z FortiGate 110D na nowym urządzeniu bądź skonfigurowanie nowego urządzenia adekwatnie jak dotychczasowy FortiGate 110D, e) Konfiguracja urządzenia i jego interfejsów, f) Konfiguracja systemu urządzenia z posiadanym środowiskiem sieciowym oraz innymi urządzeniami, g) Konfiguracja systemu, w szczególności polityk reguł, obiektów (adresów, grup, serwisów), tuneli VPN, interfejsów, routingu, h) testy konfiguracyjne i wydajnościowe środowiska, i) przekazanie dokumentacji powdrożeniowej.
8.6.25.	Testy wydajnościowe oraz funkcjonalne: a) wszystkie funkcje i parametry wydajnościowe oferowanego rozwiązania mogą być zweryfikowane przez Zamawiającego w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
8.6.26.	Serwisy i licencje Zamawiający wymaga (jeżeli dotyczy) dostawy wszystkich wymaganych licencji do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), b) Analiza typu Sandbox cloud, c) Antyspam, d) Web Filtering, e) bazy reputacyjne adresów IP/domen na okres min. 12 miesięcy.
8.6.27.	Gwarancja: min. 12 miesięcy. System musi być objęty serwisem gwarancyjnym producenta polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement).

	W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

8.7. Rozbudowa zabezpieczeń logicznych typ II

ID	Opis wymagania
8.7.1.	Zakres Przedmiotu zamówienia obejmuje Rozbudowę zabezpieczeń technicznych typ II.
8.7.2.	Przedmiotem zamówienia jest rozbudowa zabezpieczeń logicznych polegająca na zakupie/wymianie/podniesieniu wersji posiadanego przez Zamawiającego oprogramowania: posiadana licencja źródłowa przez Zamawiającego: ESET Endpoint Protection Standard Liczba stanowisk: 150 do wersji docelowej – wymaganej w ramach realizacji postępowania: **ESET PROTECT Advanced ON-PREM** liczba stanowisk: **150** wraz z odnowieniem i wsparciem technicznym na okres min. 12 miesięcy lub rozwiązanie równoważne opisane przez Zamawiającego w pkt.8.7.
8.7.3.	Zabezpieczenie techniczne typ II – oprogramowania (kompletny pakiet bezpieczeństwa) przeznaczone do ochrony stacji roboczych i serwera plików, uzupełniony o chmurowy sandboxing oraz opcję pełnego szyfrowania dysków, kontrolowany z poziomu konsoli centralnego zarządzania, dostępnej w wersji chmurowej lub lokalnej realizujący funkcje: a) zarządzania bezpieczeństwem - zdalne zarządzanie jako rozwiązanie oparte na chmurze lub wdrażane na lokalnych serwerach Zamawiającego, b) zaawansowana wielopoziomowa ochrona komputerów i maszyn wirtualnych, c) zabezpieczenia serwera plików - ochrona danych przechodzących przez wszystkie serwery w czasie rzeczywistym, d) możliwość szyfrowanie dysków systemowych, partycji lub całych urządzeń, e) proaktywna ochrona przed zagrożeniami i atakami typu zero-day dzięki analizie podejrzanych próbek w odizolowanym środowisku sandbox w chmurze lun rozwiązanie równoważne.
8.7.4.	Wymagania ogólne (zakres minimalny): a) wsparcie systemów Zamawiającego opisanych w pkt 8.8.9, b) instalacja z użyciem nowego lub istniejącego serwera bazy danych MS SQL Zamawiającego (jeżeli dotyczy), c) zabezpieczona komunikacja pomiędzy poszczególnymi modułami za pomocą certyfikatów, d) możliwość tworzenie własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: i. agent, ii. serwer zarządzający, iii. serwer proxy, e) zaimplementowany moduł zarządzania urządzeniami mobilnymi, f) wsparcie zarządzanie urządzeniami z systemem iOS i Android g) centralna konfiguracja i zarządzanie przynajmniej takimi modułami jak: ochrona

	antywirusowa, antyspyware, które działają na stacjach roboczych w sieci, h) wysłanie powiadomień przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog i) podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
8.7.5.	Ochrona stacji roboczych: a) wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, b) wbudowana technologia do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet, c) wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji, d) skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików, e) skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu, f) skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych, g) stosowanie wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku h) skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego), i) skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS, j) wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji Uwaga: Możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie k) blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: i. pamięci masowych, ii. optycznych pamięci masowych, iii. pamięci masowych Firewire, iv. urządzeń do tworzenia obrazów, v. drukarek USB, vi. urządzeń Bluetooth, vii. czytników kart inteligentnych, viii. modemów, ix. portów LPT/COM oraz urządzeń przenośnych l) blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł da podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia, m) praca w jednym z pięciu trybów: i. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

	ii. tyb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, iii. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, iv. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika, po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, v. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach, n) pełny raport na temat stacji, na której zostało zainstalowane oprogramowanie, w tym przynajmniej z: i. zainstalowanych aplikacji, ii. usług systemowych, iii. informacji o systemie operacyjnym i sprzęcie, iv. aktywnych procesów i połączeń sieciowych, v. harmonogramu systemu operacyjnego, pliku hosts, vi. sterowników o) automatyczna, inkrementacyjną aktualizację silnika detekcji p) tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne) q) skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego, r) ochrona antyspamowa dla programu pocztowego MS Outlook Zamawiającego, s) zapora osobista rozwiązania pracująca w jednym z czterech trybów: i. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, ii. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, iii. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, iv. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące, administrator musi posiada możliwość konfigurowania czasu działania trybu t) moduł bezpiecznej przeglądarki, u) automatyczne szyfrowanie przez przeglądarkę wszelkich danych wprowadzanych przez użytkownika, v) praca w bezpiecznej przeglądarce wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki, w) filtrowanie adresów URL w oparciu o co najmniej 140 kategorii i podkategorii, x) ochrona przed zagrożeniami 0-day, y) w przypadku stacji roboczych, wstrzymanie uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
8.7.6.	Ochrona serwera: a) ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami, b) wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, c) skanowanie dysków sieciowych typu NAS, d) wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący

	pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji, możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie, e) automatyczna, inkrementacyjną aktualizacja silnika detekcji, f) wykluczanie ze skanowania procesów, g) określenie typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty h) dodatkowe wymagania dla Serwerów Widnows: i. wsparcie skanowania magazynu Hyper-V, ii. skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego, iii. blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych, pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, iv. automatyczne wykrywanie usług zainstalowanych na serwerze i możliwość tworzenia dla nich odpowiednie wyjątków, v. wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych, vi. dodawanie wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP vii. ochrona przed oprogramowaniem wymuszającym okup.
8.7.7.	Szyfrowanie: a) system szyfrowania danych wspiera instalację aplikacji klienckiej w środowisku Microsoft Windows 32-bit i 64-bit, b) system szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault), c) autentykacja typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny d) szyfrowanie danych na komputerach z UEFI.

8.8. Oprogramowanie specjalistyczne typ II

ID	Opis wymagania
8.8.1.	Zakres Przedmiotu zamówienia obejmuje dostawę licencji Oprogramowania specjalistycznego typ II na warunkach określonych w SWZ.
8.8.2.	Oprogramowanie specjalistyczne typ II – licencja Microsoft Office 2021 Home & Business lub oprogramowanie równoważne tj. pakiet biurowy spełniający wymagania opisane przez Zamawiającego w pkt.8.8 - poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji oraz musi zawierać co najmniej następujące komponenty: a) edytor tekstu, b) arkusz kalkulacyjny, c) narzędzia do przygotowywania i prowadzenia prezentacji, d) program do zarządzania informacją przez użytkownika (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).
8.8.3.	Oprogramowanie specjalistyczne typ II musi umożliwiać: a) swobodne przenoszenie między stacjami roboczymi (np. w przypadku wymiany

	sprzętu) b) musi zapewniać prawo do instalacji bezpłatnych aktualizacji udostępnionych przez producenta oprogramowania Uwaga: Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu. Zamawiający nie dopuszcza dostawy licencji typu OEM, PKC.
8.8.4.	Wszystkie komponenty oferowanego pakietu biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi.
8.8.5.	Dostępna pełna polska wersja językowa interfejsu użytkownika, systemu komunikatów i podręcznej kontekstowej pomocy technicznej.
8.8.6.	Wykonywanie i edycja makr oraz kodu zapisanego w języku Visual Basic w plikach xls, xlsx oraz formuł w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013, MS Office 2016 oraz MS Office 2019 bez utraty danych oraz bez konieczności przerabiania dokumentów.
8.8.7.	Możliwość zapisywania wytworzonych dokumentów bezpośrednio w formacie PDF.
8.8.8.	Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory lub funkcjonalnie równoważną (użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się).
8.8.9.	Oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem: a) Microsoft Windows 10, b) Microsoft Office 2010, c) Microsoft Office 2013, d) Microsoft Office 2016, e) Microsoft Office 2019, f) Microsoft Windows Server 2008, g) Microsoft Windows Server 2012, h) Microsoft Windows Server 2016, i) Microsoft Windows Server 2019.
8.8.10.	Tworzenie i edycja dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: a) posiada kompletny i publicznie dostępny opis formatu, b) posiada zdefiniowany układ informacji w postaci XML zgodnie z załącznikiem 2 do 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. z 2016 r., poz. 113), c) umożliwia wykorzystanie schematów XML, d) wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES, e) możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów oprogramowania, f) możliwość automatycznego odświeżania danych pochodzących z Internetu w wytworzonych dokumentach elektronicznych, np. w arkuszu kalkulacyjnym,

	g) możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów elektronicznych pozwalających na stwierdzenie, czy dany dokument lub arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony, h) możliwość automatycznego odzyskiwania dokumentów elektronicznych w wypadku nieoczekiwanego zamknięcia aplikacji, np. w wyniku wyłączenia zasilania komputera, i) prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: .DOC, .DOCX, .XLS, .XLSX, .XLSM, .PPT, .PPTX, .MDB, .ACCDB, w tym obsługa formatowania, makr, formuł i formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013, MS Office 2016 i MS Office 2019, bez utraty danych oraz bez konieczności reformatowania dokumentów, j) automatyczne wyróżnianie i aktywowanie hiperłączy w dokumentach podczas edycji i odczytu, k) oprogramowanie zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy), l) oprogramowanie umożliwia dostosowanie dokumentów i szablonów do potrzeb urzędu oraz udostępnianie narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców, m) dostępna jest pełna dokumentacja rozwiązania w języku polskim, n) wszystkie aplikacje w pakiecie oprogramowania biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi.
8.8.11.	Edytor tekstów musi umożliwiać: a) edycję i formatowanie tekstu w języku polskim, przy czym zapewniona jest obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalność autokorekty i słownika wyrazów bliskoznacznych, b) wstawianie i formatowanie tabel i obiektów graficznych, powiększanie obiektów na cały ekran, wstawianie obrazów i klipów wideo online, prowadnice wyrównania ułatwiające zestawianie wykresów, zdjęć i diagramów z tekstem, c) wstawianie tabel i wykresów z arkusza kalkulacyjnego, w tym tabel przestawnych, d) wykonywanie korespondencji seryjnej bazującej na danych adresowych, np. pochodzących z arkusza kalkulacyjnego, bazy danych, narzędzia do zarządzania informacją prywatną, e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel, rysunków, automatyczne tworzenie spisu treści, f) określenie układu stron (pionowa/pozioma), formatowanie nagłówków i stopek stron, wydruk dokumentów, g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, h) praca zespołowa, śledzenie i porównywanie zmian wprowadzonych w dokumencie przez użytkowników, prosta adiustacja zapewniająca przejrzysty widok dokumentu z zachowaniem oznaczeń miejsc wprowadzenia śledzonych zmian, komentarze z możliwością oznaczania ich jako gotowe i dodawania odpowiedzi, i) pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, Microsoft Word 2007, Microsoft Word 2010, Microsoft Word 2013, Microsoft Word 2016 i Microsoft Word 2019, z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,

	j) otwieranie plików PDF i edytowanie ich zawartości (w tym akapitów, list, tabel), k) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, l) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go jako środowiska udostępniającego formularze bazujące na schematach XML z centralnego repozytorium wzorów dokumentów elektronicznych (o którym mowa w art. 19b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r., poz. 1114), które po wypełnieniu umożliwiają zapisanie pliku XML, m) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 27 grudnia 2011 r. w sprawie wymagań technicznych dla dokumentów elektronicznych zawierających akty normatywne i inne akty prawne, dzienników urzędowych wydawanych w postaci elektronicznej oraz środków komunikacji elektronicznej i informatycznych nośników danych (Dz. U. z 2011 r., Nr 289, poz. 1699)
8.8.12.	Arkusz kalkulacyjny musi umożliwiać: a) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, zapis wielu arkuszy kalkulacyjnych w jednym pliku, formatowanie czasu, daty i wartości finansowych z polskim formatem, tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, automatyczne polecanie wykresu odpowiedniego do wprowadzonych danych, b) wyszukiwanie i zamianę danych, wykonywanie analiz danych przy użyciu formatowania warunkowego, nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, c) tworzenie raportów tabelarycznych, d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), możliwość osadzania fragmentów arkusza na stronie sieci Web, e) obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych; narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, f) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, automatyczne polecanie sposobów podsumowania danych, korzystanie z możliwości tworzenia układu tabeli przestawnej wykorzystującej jedną lub wiele tabel z wykorzystaniem tej samej listy pól, tworzenie relacji między tabelami, tworzenie osi czasu tabeli przestawnej w celu interaktywnego filtrowania dat, g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, h) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, Microsoft Excel 2007, Microsoft Excel 2010, Microsoft Excel 2013, Microsoft Excel 2016 i Microsoft Excel 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, i) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
8.8.13.	Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a) przygotowywanie prezentacji multimedialnych, które będą prezentowane przy

	użyciu projektora multimedialnego, na monitorze lub tablecie, b) drukowanie w formacie umożliwiającym robienie notatek, c) zapisanie jako prezentacja tylko do odczytu, d) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, korzystanie z formatu panoramicznego i rozdzielczości HD, nagrywanie narracji i dołączanie jej do prezentacji, ułatwienia wyrównywania obiektów i stosowania jednakowych odstępów, e) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, f) możliwość tworzenia animacji obiektów i całych slajdów, g) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, h) pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, MS PowerPoint 2010, MS PowerPoint 2013 i MS PowerPoint 2016.
8.8.14.	Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego MS Exchange 2010/2013/2016, b) przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, c) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, d) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, automatyczne grupowanie poczty o tym samym tytule, e) wspieranie funkcji asystenta podczas nieobecności, f) 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, g) zarządzanie kalendarzem, udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, przeglądanie kalendarza innych użytkowników, h) zapraszanie uczestników na spotkania, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, i) zarządzanie listą zadań, zlecanie zadań innym użytkownikom, j) zarządzanie listą kontaktów, udostępnianie listy kontaktów innym użytkownikom, przeglądanie listy kontaktów innych użytkowników, możliwość przesyłania kontaktów innym użytkowników
8.8.15.	Ilość: 2 szt.

8.9. Stacja robocza typ II

ID	Opis wymagania
8.9.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Laptopa/laptopów na warunkach określonych w SWZ.
8.9.2.	Laptop– komputer przenośny typu notebook wykorzystywany do aplikacji biurowych i aplikacji dziedzinowych wykorzystywanych przez Zamawiającego.
8.9.3.	Procesor

	c) dedykowany do pracy w komputerach typu notebook, stosowany w układach jednoprocesorowych. osiągający min. 9000 pkt. w teście PassMark Single CPU zamieszczony na stronie: http://www.cpubenchmark.net/cpu_list.php w dniu zamieszczenia oferty SWZ na stronie Zamawiającego Uwaga: W przypadku jeżeli oferowany procesor nie jest zamieszczony na stronie http://www.cpubenchmark.net/cpu_list.php na Wykonawcy spoczywa obowiązek zamieszczenia wyników testów wydajności procesora i opublikowania parametrów wydajności procesora na powyższej stronie jednak nie później niż do dnia otwarcia złożonej oferty d) częstotliwość taktowania: min. 3GHz.
8.9.4.	Płyta główna: f) chipset zintegrowany, zaprojektowany do pracy w komputerach mobilnych dostosowany do zaoferowanego procesora, g) wyposażona w min. 2 sloty pamięci, h) zaprojektowana i wyprodukowana przez producenta komputera.
8.9.5.	Pamięć: f) zainstalowane: min. 8GB, g) typ: SODIMM DDR4, h) min. 2666Mhz. i) liczba wolnych gniazd pamięci: min. 1 szt., j) max. wielkość pamięci: min. 16GB.
8.9.6.	Zainstalowane dyski twarde: c) min. 1 szt. dysków SSD min. 256GB, d) interfejs dysku SSD: PCI-Express.
8.9.7.	Obraz i dźwięk: f) przekątna ekranu: min. 15,6", g) typ matrycy: TFT WVA, h) powierzchnia matrycy: matowa, i) rozdzielczość: min. 1920 x min. 1080, j) wbudowana karta graficzna zintegrowana z płytą główną.
8.9.8.	Inne: h) obudowa: kolor czarny i) porty USB: min. 1 x USB 2.0, j) porty USB: min. 2 x USB 3.0, k) min. 1x HDMI, l) min. 1x RJ-45, m) kamera internetowa: tak, n) głośniki: tak.
8.9.9.	Akcesoria: c) Mysz, d) Klawiatura.
8.9.10.	Komunikacja: f) LAN 10/100/1000 Mbit/s, g) Bluetooth, h) Wi-Fi 802.11a/b/g/n/ac.
8.9.11.	Zainstalowany System operacyjny (SO) pochodzący z najnowszej linii produktowej Producenta SO.

	System operacyjny (SO) musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: ee) system operacyjny nie wymaga aktywacji przez użytkownika, unikalny klucz produktu musi być umieszczony w BIOS/UEFI komputera. Upgrade Biosu (umieszczonego na stronie producenta płyty głównej) wykonanego przez Zamawiającego samodzielnie, nie może spowodować usunięcia klucza produktu zapisanego w BIOS/UEFI, ff) interfejsy użytkownika dostępne w wielu językach do wyboru - w tym Polskim i Angielskim, gg) możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji SO poprzez Internet, mechanizmem udostępnianym przez Producenta SO z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne, hh) możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez Administratora Zamawiającego, ii) wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, jj) zintegrowana z SO konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6, kk) graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, ll) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), mm) funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, nn) możliwość zarządzania stacją roboczą poprzez polityki grupowe - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność SO lub aplikacji, oo) możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania SO, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, pp) zabezpieczony hasłem hierarchiczny dostęp do SO, konta i profile użytkowników zarządzane zdalnie, qq) praca systemu w trybie ochrony kont użytkowników, rr) zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna SO, ss) system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, tt) zintegrowany z SO moduł synchronizacji komputera z urządzeniami zewnętrznymi, uu) wbudowany system pomocy w języku polskim, vv) możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących), ww) wsparcie dla IPSEC oparte na politykach - wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny, xx) wsparcie dla uwierzytelniania na bazie Kerberos v.5, yy) wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, zz) wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec, aaa) wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień

	polityk, bbb) wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach, ccc) wsparcie dla JScript i VBScript - możliwość uruchamiania interpretera poleceń, ddd) zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, eee) zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe, fff) przywracania obrazu plików systemowych do uprzednio zapisanej postaci. ggg) zintegrowanie z usługą katalogową (Active Directory MS Windows, którą posiada zamawiający) hhh) zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), WMI.
8.9.12.	Ilość: 2 szt.
8.9.13.	Gwarancja: min. 12 miesięcy gwarancji producenta w trybie on-site. Uwaga: Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.