Cyberbezpieczny Samorząd

Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Preambuła

Niniejszy dokument określa szczegółowe wymagania dotyczące dostawy, wdrożenia oraz uruchomienia oprogramowania i infrastruktury sprzętowej w ramach realizacji projektu „Cyberbezpieczny Samorząd" w Urzędzie Gminy w Gubinie.

Projekt ten jest współfinansowany w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2: Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest podniesienie poziomu cyberbezpieczeństwa jednostek samorządu terytorialnego poprzez wdrożenie zaawansowanych rozwiązań technologicznych i organizacyjnych, które zwiększają ochronę danych, minimalizują ryzyko zagrożeń cybernetycznych oraz zapewniają ciągłość działania systemów informacyjnych.

Realizacja projektu odzwierciedla strategiczne podejście do cyfryzacji administracji publicznej, mające na celu wzmocnienie zdolności samorządów lokalnych do przeciwdziałania współczesnym wyzwaniom w zakresie bezpieczeństwa cyfrowego. Wszelkie działania będą podejmowane w zgodzie z krajowymi i europejskimi standardami, w tym w zakresie interoperacyjności, dostępności oraz ochrony danych osobowych.

2. Wymagania ogólne

2.1. Równoważność oferowanych rozwiązań

W celu zachowania neutralności technologicznej i konkurencyjności Zamawiający dopuszcza zastosowanie rozwiązań równoważnych do wyspecyfikowanych. Za rozwiązanie równoważne uznaje się takie, które pod względem technologii, wydajności i funkcjonalności nie odbiega istotnie od określonych parametrów. Należy przy tym uwzględniać, że cechy unikalne dla danego rozwiązania, takie jak zastrzeżone patenty czy własnościowe technologie, nie podlegają porównaniu. Istotne jest, aby rozwiązanie równoważne zapewniało porównywalną wartość użytkową, realizując te same funkcjonalności w sposób niezakłócający integralności systemu.

Wykonawca proponujący rozwiązanie równoważne zobowiązany jest dostarczyć dokumentację potwierdzającą spełnienie wymagań funkcjonalnych Zamawiającego, w tym wyniki porównań, testów oraz opis możliwości oferowanego rozwiązania w odniesieniu do wyspecyfikowanego.

2.1.1. Oprogramowanie

Implementacja oprogramowania równoważnego musi odbyć się bez zakłóceń w bieżącej pracy Zamawiającego, obejmując migrację niezbędnych danych, szkolenie użytkowników, konfigurację systemu oraz zapewnienie gwarancji i serwisu. Wszelkie działania powinny być realizowane zgodnie z ustalonym harmonogramem i w porozumieniu z Zamawiającym.

W przypadku braku możliwości uzyskania odpowiedniego dostępu do oprogramowania firm trzecich, Zamawiający dopuszcza wymianę oprogramowania pod warunkiem, że:

a) Wykonawca dostarcza i wdraża rozwiązania zastępujące na własny koszt, zgodnie z warunkami licencjonowania określonymi w niniejszym dokumencie.

b) Migracja danych, obejmująca pełny zakres danych bieżących i archiwalnych, przeprowadzana jest na koszt Wykonawcy i zgodnie z opisem w OPZ.
c) Wykonawca zapewnia instruktaże stanowiskowe, gwarancję, serwis gwarancyjny, help desk oraz asystę techniczną umożliwiającą płynną obsługę oprogramowania przez pracowników Zamawiającego.
d) Wymiana oprogramowania nie zakłóca bieżącej pracy Zamawiającego i zapewnia ciągłość operacyjną zgodnie z obowiązującymi terminami, przepisami prawa i procedurami.
e) Uzgodnienia i konsultacje dotyczące transmisji danych odbywają się w siedzibie Zamawiającego według zatwierdzonego harmonogramu.
f) Proces migracji obejmuje pełne dane zawarte w poprzednio użytkowanym systemie.
g) Nowe rozwiązania spełniają wszystkie określone wymagania względem oprogramowania.

2.1.2. Infrastruktura sprzętowa

Jeśli w opisie przedmiotu zamówienia wskazano znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, które charakteryzują produkty lub usługi dostarczane przez konkretnego wykonawcę, co mogłoby prowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie mógł opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń, co jest uzasadnione specyfiką przedmiotu zamówienia. W takich przypadkach wszelkie odniesienia należy interpretować z dopiskiem „lub równoważne".

Gdy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, dopuszcza się rozwiązania równoważne opisywanym, a powyższe odniesienia należy rozumieć z dopiskiem „lub równoważne".

Przez rozwiązania równoważne Zamawiający rozumie sprzęt o parametrach technicznych i funkcjonalnych co najmniej równych określonym w OPZ. Wykonawca powołujący się na rozwiązania równoważne jest zobowiązany wykazać, że oferowane dostawy lub usługi spełniają wymagania Zamawiającego.

O ile nie zaznaczono inaczej, wszelkie parametry techniczne podane w OPZ należy traktować jako minimalne. Na przykład zapis: „Zainstalowane dwa procesory minimum 12-rdzeniowe klasy x86, min. 3.0GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 207 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej" należy rozumieć jako:

„Zainstalowane co najmniej dwa procesory, posiadające co najmniej 12 rdzeni, klasy x86, o taktowaniu co najmniej 3.0GHz, umożliwiające osiągnięcie wyniku co najmniej 207 w teście SPECrate2017_int_base dla oferowanego serwera, dostępnego na stronie www.spec.org w konfiguracji dwuprocesorowej".

2.1.3. Zgodność z przepisami prawa w zakresie ochrony danych i cyberbezpieczeństwa

W przypadku, gdy szczegółowy opis danego komponentu nie zawiera odrębnych wymagań w zakresie zgodności z przepisami, przyjmuje się, że wszystkie dostarczane rozwiązania oraz realizowane usługi muszą być zgodne z obowiązującym prawem, w szczególności: rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), Krajowymi Ramami Interoperacyjności (KRI), ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, a także dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (tzw. NIS2) w zakresie mającym zastosowanie. Wymagania wynikające z powyższych regulacji obejmują m.in. zapewnienie

odpowiedniego poziomu bezpieczeństwa informacji, ciągłości działania oraz odporności systemów teleinformatycznych na incydenty.

Obowiązek zapewnienia pełnej zgodności z wymienionymi regulacjami spoczywa na Wykonawcy i podlegać będzie weryfikacji na etapie odbioru przedmiotu zamówienia.

2.2. Kody CPV

48000000-8 – Pakiety oprogramowania i systemy informatyczne
48610000-7 – Systemy baz danych
48730000-4 – Pakiety oprogramowania zabezpieczającego
48732000-8 – Oprogramowanie do zarządzania tożsamością
48800000-6: Systemy informatyczne i serwery

72260000-5: Usługi powiązane z oprogramowaniem
72610000-9: Usługi wsparcia technicznego
79417000-0: Usługi doradcze w zakresie bezpieczeństwa
79131000-1 Usługi w zakresie dokumentów

80510000-2: Usługi szkoleniowe w dziedzinie informatyki
80550000-4: Usługi szkolenia w dziedzinie bezpieczeństwa

2.3. Okres gwarancji i/lub wsparcia technicznego

O ile w szczegółowym opisie przedmiotu zamówienia (OPZ) nie wskazano inaczej, Wykonawca zobowiązany jest do zapewnienia gwarancji oraz świadczenia usług wsparcia technicznego i merytorycznego (w tym wsparcia powdrożeniowego) nie krócej niż do dnia 30 czerwca 2026 r. Wymóg ten stanowi minimalny okres świadczenia wskazanych usług oraz obowiązywania gwarancji, niezależnie od daty odbioru przedmiotu zamówienia, z zastrzeżeniem zapisów szczegółowych zawartych w niniejszym OPZ.

3. Infrastruktura teleinformatyczna (obszar techniczny)

3.0.1.	Dostarczane urządzenia muszą być fabrycznie nowe, nieużywane, wolne od wad prawnych i fizycznych, pochodzić z oficjalnego kanału dystrybucyjnego producenta oraz znajdować się w okresie wsparcia producenta (co najmniej 36 miesięcy od daty dostawy).
3.0.2.	Zamawiający zastrzega, by dostarczane urządzenia nie były używane przed ich dostawą i odbiorem. 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.

3.1. Serwer wirtualizacji HCI*

3.1.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Serwera wirtualizacji HCI na warunkach określonych w SWZ.
3.1.2.	Obudowa: a) typu RACK, wysokość 2U, b) szyny umożliwiające wysunięcie serwera z szafy stelażowej, c) możliwość zainstalowania min 8 dysków SAS SSD/SATA SSD/PCIe SSD hot plug 2,5” z możliwością rozbudowy do 16 dysków, d) zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych, e) możliwość instalacji czujnika otwarcia obudowy zintegrowany z systemem i kartą zarządzającą serwera.
3.1.3.	Płyta główna: a) dwuprocesorowa, b) wyprodukowana i zaprojektowana przez producenta serwera, c) możliwość instalacji procesorów min. 86-rdzeniowych, d) zainstalowany moduł TPM 2.0 v2, e) min. 9 szt. slotów PCI Express min. generacji min. 5 Uwaga: min.4 fizyczne złącza o prędkości x16, min.4 fizyczne złącza o prędkości x8 Full height, f) min. 32 sztuki gniazd pamięci RAM, g) obsługa min. 8TB pamięci RAM DDR5, h) wsparcie dla technologii (zakres minimalny): i. Memory Scrubbing, ii. ECC, iii. SDDC.
3.1.4.	Procesory: a) zainstalowane: min. 2 szt. 8-rdzeniowe, b) architektura x86_64, c) taktowanie bazowe: min. 3,5 GHz, d) pamięć cache: min. 48 MB, Osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 403 pkt, dla zainstalowanych dwóch procesorów. Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla oferowanego serwera.
3.1.5.	Pamięć RAM: a) zainstalowane: min. 512GB, b) typ: DDR5 Registered min. 6400MT/s,

	Uwaga: Pamięci obsadzone w sposób gwarantujący najwyższą możliwą wydajność.
3.1.6.	Zainstalowane dyski twarde: a) min. 2 szt. dyski PCIe M.2 min 480GB wraz z dedykowanym kontrolerem sprzętowym RAID 0/1, b) min. 6 szt. dysków PCIe SSD hot plug o pojemności min 1,92TB.
3.1.7.	Interfejsy zintegrowane: a) zintegrowana karta graficzna ze złączem VGA, b) min. 2 szt. portów USB 3.0, c) min. 1 szt. portów USB wewnętrzny, d) możliwość instalacji min. 1 szt. portu serial RS232: opcjonalnie, Uwaga: Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
3.1.8.	Interfejsy sieciowe: a) Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express: i. 1x 1Gbit Base-T ii. 2x 10Gbit SFP+ z modułami MMF LC, Uwaga: Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji w slotach PCIe.
3.1.9.	Zasilanie i chłodzenie: a) redundantne zasilacze hotplug o sprawności min. 96% (tzw. klasa Titanium) o mocy min. 900W: 2 szt., b) redundantne wentylatory hotplug.
3.1.10.	Zarządzanie: a) informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: i. karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, ii. procesory CPU, iii. pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, iv. status karty zarządzającej serwera, v. wentylatory, vi. bateria podtrzymująca ustawienia BIOS płyty głównej, vii. zasilacze, b) zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: i. niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera, ii. dedykowana karta LAN 1Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym lub inne rozwiązanie równoważne, iii. dostęp poprzez przeglądarkę Web, SSH, iv. zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii, v. zarządzanie alarmami (zdarzenia poprzez SNMP), vi. możliwość przejęcia konsoli tekstowej, vii. możliwość przekierowania konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM),

	viii. obsługa serwerów proxy (autentykacja), ix. obsługa VLAN, x. możliwość konfiguracji parametru Max. Transmission Unit (MTU), xi. wsparcie dla protokołu SSDP, xii. Obsługa protokołów TLS min. 1.2 (zalecane 1.3), xiii. obsługa protokołu LDAP, xiv. synchronizacja czasu poprzez protokół NTP, xv. możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej, c) dostarczone oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające: i. konfigurację kontrolera RAID, ii. instalację systemów operacyjnych, iii. zdalne zarządzanie, iv. 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); d) wbudowana karta zarządzającą (lub zainstalowana) pamięć flash lub rozwiązanie równoważne dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN, Uwaga: Serwer musi posiadać możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera.
3.1.11.	Wymagane wsparcie dla systemów SSO (zakres minimalny): a) rozwiązanie musi współpracować z systemami serwerowymi i usługami katalogowymi klasy enterprise wykorzystywanymi przez Zamawiającego (SSO zgodnie z pkt 3.9), w tym z systemami z rodziny Windows Server oraz dystrybucjami Linux klasy enterprise i popularnymi hypervisorami typu 1 (np. Windows Server, RHEL/Oracle Linux, VMware ESXi - lub rozwiązania równoważne).
3.1.12.	Pozostałe wymagania: a) elementy, z których zbudowane jest serwer muszą być produktami producenta tego serwera lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA, b) serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego wymagane oświadczenie wykonawcy lub producenta z chwilą dostawy.
3.1.13.	Oprogramowanie SSO: zainstalowane Oprogramowanie systemowe typ I (SSO) zgodnie z wymaganiami opisanymi przez Zamawiającego w ptk.3.9.
3.1.14.	Ilość: 1 szt. Z zainstalowanym SSO zgodnie z pkt.3.9. Wraz z SSO należy dostarczyć 45 licencji dostępowych (CAL) na użytkownika.
3.1.15.	Gwarancja: Serwis gwarancyjny producenta przez okres: min. zgodnie z pkt.2.3 w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. a) naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis, b) możliwość zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu, c) bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dla oferowanego serwera przez cały okres gwarancji (min. zgodnie z pkt 2.3)

	Uwaga: Jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniony w ofercie Wykonawcy, d) możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.
3.1.16.	Dokumentacja, inne a) ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, b) możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.
3.1.17.	Do czynności Wykonawcy w ramach montażu i uruchomienia serwera należy: a) ustalenie z Zamawiającym terminu przeprowadzenia prac, b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia, c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce), d) instalacja urządzenia zgodnie ze specyfikacjami produktu, w tym m.in. zamontowanie w szafach dystrybucyjnych, e) instalacja SSO zgodnie z pkt.3.9, f) oznakowanie sprzętu naklejką, g) zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego.
3.1.18.	Na potwierdzenie, że oferowany Serwer wirtualizacji HCI spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć do oferty następujące dokumenty: a) opis proponowanego rozwiązania potwierdzający, że oferowany Serwer wirtualizacji HCI spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań. b) opis proponowanego rozwiązania potwierdzający, że oferowany SSO spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, rodzaju licencji oferowanego rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.
3.1.19.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: a) dostawa: formalnemu odbiorowi podlega dostawa w ilościach określonych w pkt.3.1.14, b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzeń zgodnie z wykazem czynności określonym w pkt.3.1.17.

3.2. Serwer logów*

3.2.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Serwera logów na warunkach określonych w SWZ.
3.2.2.	Obudowa: a) typu RACK, wysokość 2U, b) szyny umożliwiające wysunięcie serwera z szafy stelażowej, c) możliwość zainstalowania min 8 dysków SAS SSD/SATA SSD/PCIe SSD hot plug 2,5” z możliwością rozbudowy do 16 dysków, d) zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych, możliwość instalacji czujnika otwarcia obudowy zintegrowany z systemem i kartą zarządzającą serwera.
3.2.3.	Płyta główna: a) dwuprocesorowa,

	b) wyprodukowana i zaprojektowana przez producenta serwera, c) możliwość instalacji procesorów min. 86-rdzeniowych, d) zainstalowany moduł TPM 2.0 v2, e) min. 9 szt. slotów PCI Express min. generacji min. 5 Uwaga: min.4 fizyczne złącza o prędkości x16, min.4 fizyczne złącza o prędkości x8 Full height, f) min. 32 sztuki gniazd pamięci RAM, g) obsługa min. 8TB pamięci RAM DDR5, h) wsparcie dla technologii (zakres minimalny): i. Memory Scrubbing, ii. ECC, iii. SDDC.
3.2.4.	Procesory: a) zainstalowane: min. 2 szt. 8-rdzeniowe, b) architektura x86_64, c) taktowanie bazowe: min. 3,5 GHz, d) pamięć cache: min. 48 MB, Osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 403 pkt, dla zainstalowanych dwóch procesorów. Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla oferowanego serwera.
3.2.5.	Pamięć RAM: a) zainstalowane: min. 512GB, b) typ: DDR5 Registered min. 6400MT/s, Uwaga: Pamięci obsadzone w sposób gwarantujący najwyższą możliwą wydajność.
3.2.6.	Zainstalowane dyski twarde: a) min. 2 szt. dyski PCIe M.2 min 480GB wraz z dedykowanym kontrolerem sprzętowym RAID 0/1, b) min. 6 szt. dysków PCIe SSD hot plug o pojemności min 1,92TB.
3.2.7.	Interfejsy zintegrowane: a) zintegrowana karta graficzna ze złączem VGA, b) min. 2 szt. portów USB 3.0, c) min. 1 szt. portów USB wewnętrzny, d) możliwość instalacji min. 1 szt. portu serial RS232: opcjonalnie, Uwaga: Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
3.2.8.	Interfejsy sieciowe: a) Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express: i. 1x 1Gbit Base-T ii. 2x 10Gbit SFP+ z modułami MMF LC, Uwaga: Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji w slotach PCIe.
3.2.9.	Zasilanie i chłodzenie: a) redundantne zasilacze hotplug o sprawności min. 96% (tzw. klasa Titanium) o mocy min. 900W: 2 szt.,

	b) redundantne wentylatory hotplug.
3.2.10.	Zarządzanie: a) informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: i. karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, ii. procesory CPU, iii. pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, iv. status karty zarządzającej serwera, v. wentylatory, vi. bateria podtrzymująca ustawienia BIOS płyty głównej, vii. zasilacze, b) zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: i. niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera, ii. dedykowana karta LAN 1Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym lub inne rozwiązanie równoważne, iii. dostęp poprzez przeglądarkę Web, SSH, iv. zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii, v. zarządzanie alarmami (zdarzenia poprzez SNMP), vi. możliwość przejęcia konsoli tekstowej, vii. możliwość przekierowania konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM), viii. obsługa serwerów proxy (autentykacja), ix. obsługa VLAN, x. możliwość konfiguracji parametru Max. Transmission Unit (MTU), xi. wsparcie dla protokołu SSDP, xii. Obsługa protokołów TLS min. 1.2 (zalecane 1.3), xiii. obsługa protokołu LDAP, xiv. synchronizacja czasu poprzez protokół NTP, xv. możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej, c) dostarczone oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające: i. konfigurację kontrolera RAID, ii. instalację systemów operacyjnych, iii. zdalne zarządzanie, iv. 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); d) wbudowana karta zarządzającą (lub zainstalowana) pamięć flash lub rozwiązanie równoważne dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN, Uwaga: Serwer musi posiadać możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera.
3.2.11.	Wymagane wsparcie dla systemów SSO (zakres minimalny):

	a) rozwiązanie musi współpracować z systemami serwerowymi i usługami katalogowymi klasy enterprise wykorzystywanymi przez Zamawiającego (SSO zgodnie z pkt 3.9), w tym z systemami z rodziny Windows Server oraz dystrybucjami Linux klasy enterprise i popularnymi hypervisorami typu 1 (np. Windows Server, RHEL/Oracle Linux, VMware ESXi - lub rozwiązania równoważne).
3.2.12.	Pozostałe wymagania: a) elementy, z których zbudowane jest serwer muszą być produktami producenta tego serwera lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA, b) serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego wymagane oświadczenie wykonawcy lub producenta z chwilą dostawy.
3.2.13.	Oprogramowanie SSO: zainstalowane Oprogramowanie systemowe typ I (SSO) zgodnie z wymaganiami opisanymi przez Zamawiającego w ptk.3.9.
3.2.14.	Ilość: 1 szt. Z zainstalowanym SSO zgodnie z pkt.3.9.
3.2.15.	Gwarancja: Serwis gwarancyjny producenta przez okres: min. zgodnie z pkt.2.3 w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. a) naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis, b) możliwość zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu, c) bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera Uwaga: Jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniony w ofercie Wykonawcy, d) możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.
3.2.16.	Dokumentacja, inne a) ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, b) możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.
3.2.17.	Do czynności Wykonawcy w ramach montażu i uruchomienia serwera należy: a) ustalenie z Zamawiającym terminu przeprowadzenia prac, b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia, c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce), d) instalacja urządzenia zgodnie ze specyfikacjami produktu, w tym m.in. zamontowanie w szafach dystrybucyjnych, e) instalacja SSO zgodnie z pkt.3.9, f) oznakowanie sprzętu naklejką, g) zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego.
3.2.18.	Na potwierdzenie, że oferowany Serwer logów spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć do oferty następujące dokumenty: a) opis proponowanego rozwiązania potwierdzający, że oferowany Serwer logów spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego

	rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań. b) opis proponowanego rozwiązania potwierdzający, że oferowany SSO spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, rodzaju licencji oferowanego rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.
3.2.19.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: a) dostawa: formalnemu odbiorowi podlega dostawa w ilościach określonych w pkt.3.2.14, b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzeń zgodnie z wykazem czynności określonym w pkt.3.2.17.

3.3. Agregat prądotwórczy typ I*

3.3.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Agregatu prądotwórczego typ I na warunkach określonych w SWZ, zwanego dalej „Agregatem prądotwórczym typ I" lub „Systemem zasilania rezerwowego". Przedmiot zamówienia obejmuje: a) dostawę, transport, rozładunek, posadowienie, montaż, b) uruchomienie, konfigurację i integrację z układem SZR, c) przeprowadzenie testów funkcjonalnych oraz szkolenia obsługi w zakresie eksploatacji dostarczonego trójfazowego zespołu prądotwórczego, stanowiącego źródło zasilania rezerwowego dla infrastruktury Zamawiającego, d) ~~wykonanie oraz montaż ogrodzenia stanowiska agregatu zgodnie z pkt 3.3.8~~. Uwaga: Zamawiający dopuszcza rozwiązania równoważne pod względem parametrów technicznych, funkcjonalnych i jakościowych, spełniające wymagania określone w niniejszym opisie, z zachowaniem zasad określonych w ustawie Prawo zamówień publicznych. Posadowienie na fundamencie wykonanym przez Zamawiającego.
3.3.2.	Wymagane minimalne parametry techniczne Agregatu prądotwórczego typ I (zwany zespołem): a) zespół prądotwórczy napędzany silnikiem spalinowym wysokoprężnym (olej napędowy), chłodzonym cieczą / płynem niezamarzającym, z wtryskiem bezpośrednim, przystosowany do pracy przy prędkości obrotowej ok. 1500 obr./min oraz wyposażony w układ regulacji obrotów silnika w standardzie elektronicznym, b) zespół wykonany w obudowie przystosowanej do pracy na zewnątrz, wyciszonej (dźwiękochłonnej), ograniczającej emisję hałasu zgodnie z obowiązującymi przepisami dotyczącymi poziomu mocy akustycznej dla zespołów prądotwórczych eksploatowanych na zewnątrz (m.in. dyrektywa 2005/88/WE lub równoważna). Uwaga: Poziom hałasu agregatu w obudowie wyciszonej musi spełniać wymagania dla urządzeń eksploatowanych na zewnątrz wynikające z właściwych przepisów, Wykonawca potwierdzi spełnienie tego wymagania w dokumentacji technicznej oferowanego urządzenia. c) Moc maksymalna awaryjna (moc rezerwowa wg ISO 8528, określana jako L.T.P. / E.S.P. lub równoważnie „Emergency/Standby Power"): min. 44 kVA / 35 kW

	Uwaga: Moc mierzona przy 400V, 50Hz, w warunkach referencyjnych (temperatura otoczenia do 27°C, wysokość do 1000 m n.p.m.). Praca w tym trybie nie dłużej niż 500 godzin rocznie i bez dopuszczalnego przeciążania. d) Moc znamionowa podstawowa (P.R.P. – Prime Power wg ISO 8528): min. 40 kVA / 32 kW przy 400 V, 50 Hz Uwaga: Dopuszcza się obciążenie do 10% powyżej mocy P.R.P. maksymalnie przez 1 godzinę na każde 12 godzin pracy, zgodnie z normą ISO 8528 lub równoważną. e) Napięcie znamionowe pracy: 400 V / 230 V (układ trójfazowy 50 Hz). f) Częstotliwość znamionowa: 50 Hz, g) Agregat musi być przystosowany do współpracy z układem SZR dostarczanym w ramach Przedmiotu Zamówienia Uwaga: tj. zapewniać stabilne napięcie i częstotliwość w zakresie akceptowalnym dla UPS-ów klasy on-line / double conversion (wymagany elektroniczny regulator napięcia AVR oraz stabilizacja częstotliwości). h) Paliwo: olej napędowy spełniający wymagania EN 590 lub równoważnej normy jakości paliw do silników wysokoprężnych. i) Rozruch automatyczny sterowany sygnałem beznapięciowym z układu SZR / sterownika (automatyczny start przy zaniku napięcia sieci podstawowej). Uwaga: Zespół dostarczany z kompletnym panelem sterowania przystosowanym do pracy automatycznej i współpracy z SZR (patrz pkt 3.3.3 oraz 3.3.4.). j) Grzałka bloku silnika sterowana termostatem (utrzymanie temperatury postojowej silnika dla szybkiego startu w warunkach obniżonych temperatur), k) Zabezpieczenie prądnicowe: wyłącznik mocy 3P pełniący funkcję zabezpieczenia zwarciowego i umożliwiający awaryjne odłączenie zespołu (wyłącznik główny odbioru mocy). l) Automatyczna ładowarka/ładowarka buforowa akumulatorów rozruchowych oraz dostarczone akumulatory rozruchowe o pojemności min. 100 Ah lub równoważnej, zapewniające pewny start. m) Elektroniczny regulator napięcia prądnicy (AVR) zapewniający stabilizację napięcia wyjściowego w granicach ±0,25% lub lepiej, przy zmianach obciążenia (bezszczotkowa prądnica synchroniczna, klasa izolacji min. H, stopień ochrony min. IP23 lub równoważnie). n) Zespół dostarczany z wibroizolatorami, kompensatorem wydechu i tłumikiem spalin, kompletną instalacją paliwową oraz szafą potrzeb własnych i odbioru mocy. o) Zbiornik paliwa zintegrowany w ramie agregatu, o pojemności zapewniającej nieprzerwaną pracę przez co najmniej 8 godzin przy obciążeniu 75–80% mocy znamionowej P.R.P. p) pojemność użytkowa zbiornika: min. 180 litrów. q) Zasilacz/układ buforowy do ładowania akumulatorów rozruchowych (funkcja podtrzymania stanu gotowości).

	r) Sterownik/układ nadzoru musi umożliwiać lokalny podgląd podstawowych parametrów pracy zespołu oraz sygnalizację alarmów. Funkcje zdalnego monitoringu (np. LAN/Modbus/RS485/Ethernet/GPRS) są dopuszczalne jako opcja, jeżeli wynikają z konfiguracji oferowanego rozwiązania. Uwaga: W przypadku zaoferowania funkcji zdalnego monitoringu Zamawiający wymaga zapewnienia podglądu historii zdarzeń i parametrów bieżących pracy agregatu. Uwaga: Przedmiot Zamówienia obejmuje dostawę Agregatu prądotwórczego typ I wraz ze wszystkimi niezbędnymi płynami eksploatacyjnymi oraz zapasem paliwa umożliwiającym wykonanie wymaganych testów obciążeniowych.
3.3.3.	Układ SZR / układy przełączające: a) Zamawiający wymaga dostawy, montażu i konfiguracji samoczynnego załączania rezerwy (SZR) - układ stycznikowy 3-fazowy (3P) o prądzie znamionowym min. 70 A, dostosowany do parametrów dostarczonego agregatu prądotwórczego typ I, przystosowany do montażu w pomieszczeniu Zamawiającego (dopuszcza się rozwiązanie równoważne do montażu na zewnątrz), b) SZR ma zapewnić automatyczne przełączenie zasilania z sieci podstawowej na agregat oraz powrót na zasilanie podstawowe po jego przywróceniu, c) SZR musi współpracować ze sterownikiem opisanym w pkt 3.3.4 oraz udostępniać sygnał rozruchu/stop dla agregatu. Uwaga: SZR jest elementem dostawy.
3.3.4.	Sterownik agregatu / sterownik SZR: a) interfejs graficzny umożliwiający lokalny odczyt parametrów i obsługę serwisową (inteligentny/mikroprocesorowy sterownik klasy AMF/ATS lub równoważny), b) zegar czasu rzeczywistego z podtrzymaniem, c) obsługa automatycznego startu agregatu oraz automatycznego przełączenia zasilania w trybie rezerwowym. d) Pomiar i prezentacja co najmniej następujących wielkości: i. prądy fazowe (3 fazy), ii. napięcie sieci zasilającej, iii. napięcie generatora agregatu, iv. moc czynna, bierna i pozorna, v. napięcie akumulatora rozruchowego, vi. poziom paliwa w zbiorniku. e) licznik energii generatora oraz licznik czasu pracy (motogodziny), f) rejestr zdarzeń/awarii (min. 100 wpisów lub równoważnie), g) możliwość zdalnego nadzoru oraz przesyłania powiadomień alarmowych o błędach/awariach - o ile funkcjonalność ta wynika z konfiguracji oferowanego rozwiązania, Uwaga: Jeżeli Wykonawca zaoferuje funkcję zdalnego nadzoru, Zamawiający wymaga zapewnienia dostępu do historii zdarzeń oraz możliwości przesyłania powiadomień alarmowych. h) zabezpieczenia generatora (częstotliwość, napięcie, asymetria faz, przeciążenie).
3.3.5.	Obudowa:

	a) Obudowa wyciszona, dźwiękochłonna, przystosowana do trwałej pracy na zewnątrz, odporna na warunki atmosferyczne, b) wykonana z blach stalowych zabezpieczonych antykorozyjnie (np. alucynk, malowanie proszkowe lub rozwiązanie równoważne zapewniające trwałość antykorozyjną min. 5 lat), c) obudowa powinna być wyposażona w szafę potrzeb własnych i odbioru mocy oraz przycisk awaryjnego zatrzymania z sygnalizacją akustyczną awarii. Uwaga: Agregat w obudowie musi spełniać wymagania w zakresie emisji hałasu dla urządzeń pracujących na zewnątrz wynikające z dyrektywy 2005/88/WE lub norm równoważnych.
3.3.6.	Wymagane posadowienie na utwardzonym i wypoziomowanym podłożu np. płyta fundamentowa. Uwaga: Przedmiot Zamówienia nie obejmuje zaprojektowanie i wykonanie płyty fundamentowej
3.3.7.	Wymagane zabezpieczenia i mechanizmy ochronne: a) Zabezpieczenie przed nadmierną temperaturą silnika, b) Zabezpieczenie przed zbyt niskim ciśnieniem oleju, c) Zabezpieczenie przed przekroczeniem prędkości obrotowej (overspeed), d) Zabezpieczenie przed zbyt niską prędkością obrotową (underspeed), e) Zabezpieczenie przed zbyt wysokim i przed zbyt niskim napięciem wyjściowym generatora, f) Zabezpieczenie przeciążeniowe generatora, g) Możliwość awaryjnego wyłączenia agregatu z poziomu przycisku bezpieczeństwa.
3.3.8.	~~Wytyczne dot. ogrodzenia:~~ ~~a) Rodzaj: Panelowe,~~ ~~b) Szerokość: zgodnie z projektem Wykonawcy,~~ ~~c) Wysokość: min. 170cm,~~ ~~d) Kolor: zielony,~~ ~~e) Ocynk elektrolityczny: tak,~~ ~~f) Trwałość powłoki antykorozyjnej: min. 5 lat ,~~ ~~g) Powłoka antykorozyjna: nawierzchniowa proszkowa,~~ ~~h) Rodzaj profilu belki poprzecznej: pełny,~~ ~~i) Rodzaj materiału wypełnienia: stal,~~ ~~j) Wymiar oczka: max. 50 x max. 200 mm,~~ ~~k) Typ materiału belki poprzecznej: stal.~~ ~~Uwaga:~~ ~~Zamawiający wymaga montażu 1 szt. furtki wejściowej zamykanej (zamek patentowy) zgodnie z projektem Wykonawcy stanowiącej element/moduł zaprojektowanego systemu ogrodzeniowego (szerokość: min. 100cm, wysokość: zgodnie z wysokością ogrodzenia panelowego). Wersję furtki należy dobrać w zależności od potrzeb i uzgodnień z Zamawiającym (lewa/prawa).~~
3.3.9.	Ilość: 1 szt.
3.3.10.	Gwarancja: min. zgodnie z pkt.2.3.
3.3.11.	Na potwierdzenie, że oferowany Agregat prądotwórczy typ I (wraz z układem SZR) spełnia wymagania określone przez Zamawiającego, Wykonawca zobowiązany jest dołączyć następujące dokumenty: a) opis proponowanego rozwiązania potwierdzający, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego

	urządzenia wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.
3.3.12.	W zakresie instalacji i konfiguracji urządzeń Wykonawca powinien zapewnić: a) uzgodnienie z Zamawiającym terminu dostawy i montażu, b) transport na miejsce wskazane przez Zamawiającego, rozładunek i posadowienie agregatu na płycie fundamentowej Zamawiającego, c) podłączenie agregatu do instalacji elektrycznej Zamawiającego, w tym do dostarczonego układu SZR, wraz z wykonaniem wymaganych przyłączy mocy oraz przewodów sterujących rozruchem/stopem, d) napełnienie układów eksploatacyjnych (olej silnikowy, płyn chłodzący) oraz zatankowanie paliwa w ilości niezbędnej do przeprowadzenia testów odbiorowych (uruchomienie w trybie pracy rezerwowej pod obciążeniem), e) wykonanie prób funkcjonalnych obejmujących co najmniej: i. automatyczny rozruch agregatu po zaniku napięcia sieci podstawowej, ii. automatyczne przełączenie zasilania na agregat i powrót na zasilanie podstawowe po jego przywróceniu, iii. weryfikację stabilności napięcia i częstotliwości przy obciążeniu, iv. sprawdzenie poprawności działania zabezpieczeń oraz sygnałów alarmowych sterownika, v. rejestrację i przekazanie Zamawiającemu wyników testów (protokół odbioru), f) przeszkolenie wskazanych pracowników Zamawiającego w zakresie podstawowej obsługi, bezpiecznego uruchamiania/wyłączania, kontroli poziomu paliwa i podstawowych komunikatów alarmowych sterownika (szkolenie na miejscu, w ramach uruchomienia). g) przekazanie dokumentacji techniczno-ruchowej, instrukcji obsługi PL/EN, schematów elektrycznych przyłączenia, certyfikatów zgodności oraz protokołów z prób funkcjonalnych.
3.3.13.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: a) dostawa: formalnemu odbiorowi podlega dostawa do Zamawiającego w ilościach określonych w pkt.3.3.9, b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzenia u Zamawiającego zgodnie z wykazem czynności określonym w pkt.3.3.12.

3.4. Urządzenie typu UPS moc. 20kVA*

3.4.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją urządzenia typu UPS o mocy 20kVA/20kW zwanego dalej UPS typ I na warunkach określonych w SWZ.
3.4.2.	Klasa produktu: true on-line, podwójne przetwarzanie energii.
3.4.3.	Moc znamionowa: min. 20 000 VA / 20 000 W
3.4.4.	Architektura/Technologia: beztransformatorowa o podwójnej konwersji. Uwaga: UPS musi umożliwiać niezależne zasilanie toru prostownika i toru bypassu lub rozwiązanie równoważne zapewniające ciągłość pracy i bezpieczeństwo zasilania. Wymagana współpraca z Agregatem prądotwórczym typ I (pk.3.3).
3.4.5.	Konfiguracja wejścia/wyjścia: 3:3.
3.4.6.	Napięcie wejściowe: 400 VAC 3F + N.

3.4.7.	Tolerancja napięcia wejściowego przy obciążeniu 100% (bez przechodzenia na baterie): min. 320 – min. 460 Vac (L-L).
3.4.8.	Wyjściowy współczynnik mocy (PF): 1.0.
3.4.9.	Współczynnik mocy wejściowej: >= min 0,95 przy pełnym obciążeniu.
3.4.10.	Zakres częstotliwości wejściowej: od min. 40Hz do min. 70Hz.
3.4.11.	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%: min. >= 95%.
3.4.12.	Napięcie wyjściowe trójfazowe: 400 VAC 3F + N.
3.4.13.	Częstotliwość wyjściowa: 50/60Hz.
3.4.14.	Czas podtrzymania: min. 10 minut przy obciążeniu 16kW.
3.4.15.	Żywotność akumulatorów: min. 3 - 5 lat (wg EUROBAT) Uwaga: Baterie umieszczone w zasilaczu UPS.
3.4.16.	Komunikacja i zarządzanie: a) USB oraz RS232 w standardzie, b) Modbus RTU - wymagany (wbudowany lub realizowany poprzez moduł/kartę komunikacyjną), c) możliwość instalacji karty sieciowej SNMP (wbudowanej lub w postaci modułu rozszerzającego), d) wyjścia bezpotencjałowe do sygnalizacji stanów alarmowych: opcjonalnie.
3.4.17.	Inne: a) interfejs EPO (do wyłącznika ppoż.): Tak, b) diagnostyka parametrów urządzenia UPS i baterii: Tak, c) zintegrowany lub zewnętrzny serwisowy przełącznik obejściowy (by-pass): wymagany.
3.4.18.	Ilość: 1 szt.
3.4.19.	Gwarancja: min. zgodnie z pkt.2.3.
3.4.20.	Na potwierdzenie, że oferowany UPS typ I spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć następujące dokumenty: a) opis proponowanego rozwiązania potwierdzający, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego urządzenia wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.
3.4.21.	W zakresie instalacji i konfiguracji urządzeń Wykonawca powinien zapewnić: a) ustalenie z Zamawiającym terminu przeprowadzenia prac, b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia, c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce), d) fizyczną instalację urządzeń i podłączenie do zasilania oraz wymaganego okablowania, e) konfigurację urządzenia zgodnie z wytycznymi Zamawiającego, która obejmuje: i. połączenie z istniejącą infrastrukturą elektryczną, ii. Testy funkcjonalne obejmujące: ▪ uruchomienie UPS typ I, ▪ kalibrację i konfigurację parametrów systemowych, iii. weryfikacja działania baterii oraz obciążenia, f) dostarczenie certyfikatu zgodności oraz dokumentacji technicznej.
3.4.22.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: a) dostawa: formalnemu odbiorowi podlega dostawa do Zamawiającego w ilościach określonych w pkt.3.4.18,

	b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzenia u Zamawiającego zgodnie z wykazem czynności określonym w pkt.3.4.21.

3.5. Urządzenie klasy UTM*

3.5.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją urządzenia typu UTM (Unified Threat Management) na warunkach określonych w SWZ zwanym dalej systemem lub systemem bezpieczeństwa.
3.5.2.	Klasa produktu: UTM (Unified Threat Management).
3.5.3.	Zintegrowany system bezpieczeństwa (UTM) ma stanowić jedno urządzenie spełniające wymagania funkcjonalne i wydajnościowe określone w pkt 3.5.4 - 3.5.13 oraz 3.5.14 (parametry sprzętowe), niezależnie od dostawcy łącza. Uwaga: W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Jeżeli realizacja wymagań wymaga dostarczenia odrębnej(-ych) licencji to dostawa licencji stanowi Przedmiot Zamówienia.
3.5.4.	Zapora Korporacyjna (Firewall) a) Firewall klasy Stateful Inspection. b) obsługa translacji adresów NAT n:1, NAT 1:1 oraz PAT, c) możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). d) Interface (GUI) musi umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów, administrator musi mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie, e) administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia, f) możliwość filtrowania jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac, g) administrator musi możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall, h) edytor reguł firewall musi posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł, i) rozwiązanie musi umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos, j) możliwość wskazania trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego), k) rozwiązanie musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
3.5.5.	Intrusion Prevention System (IPS) a) system detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe, b) moduł IPS musi być integralną częścią oferowanego rozwiązania UTM (wbudowany lub dostarczony jako komponent licencjonowany), objęty wsparciem producenta rozwiązania UTM i aktualizowany w całym okresie wsparcia, dopuszcza się wykorzystanie silnika/sygnatur IPS pochodzących od podmiotów trzecich, o ile zapewniona jest pełna

	integracja z urządzeniem, automatyczne aktualizacje oraz brak konieczności zakupu dodatkowego sprzętu, c) moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń, d) administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS, e) moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia, f) rozwiązanie musi umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS, g) administrator musi mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP, h) rozwiązanie musi umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0, i) rozwiązanie musi zapewniać automatyczną aktualizację sygnatur kontekstowych, j) moduł IPS musi umożliwiać analizę i ochronę ruchu w protokołach przemysłowych oraz specjalistycznych, wykorzystywanych w środowiskach OT/ICS, w zakresie funkcjonalnie równoważnym do obsługi protokołów takich jak m.in. Modbus, S7, EtherNet/IP, CIP, OPC UA, BACnet/IP, IEC 60870-5-104, IEC 61850 lub innych równoważnych technologii stosowanych w infrastrukturze przemysłowej.
3.5.6.	Kształtowanie pasma (traffic shaping) a) rozwiązanie musi umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma, b) ograniczenie pasma lub priorytetyzacja reguły firewall musi być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP, c) rozwiązanie musi umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring), d) rozwiązanie musi umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
3.5.7.	Ochrona antywirusowa oraz Antyspam a) Rozwiązanie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików z wykorzystaniem mechanizmu sandboxing (lokalnego i/lub chmurowego). W przypadku sandboxingu chmurowego przetwarzanie danych ma odbywać się na terenie EOG (UE/EFTA) lub w Polsce, z zapewnieniem zgodności z RODO (w tym możliwość przedstawienia informacji o lokalizacji przetwarzania i podstawie powierzenia). Dopuszcza się realizację usługi przez producenta rozwiązania lub przez jego podwykonawcę/partnera technologicznego Uwaga: Nie dopuszcza się, aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. b) skaner antywirusowy może być dostarczany przez producenta rozwiązania lub przez podmiot trzeci (np. podwykonawcę/partnera technologicznego) - w każdym przypadku musi być w pełni zintegrowany z rozwiązaniem i objęty jego wsparciem oraz aktualizacjami, c) administrator musi mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź - gdy analiza skanerem antywirusowym została zakończona błędem, d) skaner antywirusowy musi być rozwiązaniem komercyjnym, powszechnie stosowanym na rynku, utrzymywanym i aktualizowanym (automatyczne aktualizacje), z potwierdzoną skutecznością (np. raporty niezależnych testów lub równoważne potwierdzenie producenta), e) administrator musi mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym,

	f) administrator musi mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji, g) rozwiązanie musi posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM), h) ochrona antyspam ma działać w oparciu o: i. białe/czarne listy, ii. DNS RBL, iii. skaner heurystyczny, i) w przypadku ochrony w oparciu o DNS RBL administrator musi mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia, j) wpis w nagłówku wiadomości zaklasyfikowanej jako spam musi być w formacie zgodnym z formatem programu Spamassassin.
3.5.8.	Wirtualne Sieci Prywatne (VPN) a) rozwiązanie musi umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny - lokalizacja) lub site-to-site (lokalizacja-lokalizacja), b) rozwiązanie ma wspierać co najmniej następujące typy sieci VPN: i. PPTP VPN, ii. IPSec VPN, iii. SSL VPN. c) SSL VPN musi działać w trybie tunelu, d) producent urządzenia musi umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. e) klient SSL VPN musi być dostępny z poziomu portalu uwierzytelniania (captive portal) f) rozwiązanie musi umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover), g) rozwiązanie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf, h) rozwiązanie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
3.5.9.	Filtr dostępu do stron WWW a) rozwiązanie musi posiadać wbudowany filtr URL, b) filtr URL musi działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering musi posiadać miliony sklasyfikowanych stron internetowych, c) klasyfikacja URL musi być realizowana w oparciu o aktualizowaną bazę klasyfikacji dostarczaną w ramach wsparcia producenta rozwiązania (online i/lub offline - dopuszcza się komunikację z serwerami producenta lub lokalną bazę aktualizowaną automatycznie), d) Administrator ma mieć możliwość dodawania własnych kategorii URL. e) administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: i. blokowanie dostępu do adresu URL, ii. zezwolenie na dostęp do adresu URL, iii. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. f) administrator musi mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony, g) strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych, h) filtr URL musi uwzględniać komunikację po protokole HTTPS, i) możliwość identyfikacji i blokowania przesyłanych danych z wykorzystaniem typu MIME, j) możliwość stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane, k) możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

3.5.10.	Uwierzytelnianie a) możliwość uwierzytelniania użytkowników co najmniej w oparciu o: i. lokalną bazę użytkowników (wewnętrzny LDAP), ii. zewnętrzną bazę użytkowników (zewnętrzny LDAP), iii. usługę katalogową zgodną z LDAP/Kerberos/AD (np. Active Directory) lub rozwiązanie równoważne zapewniające centralne zarządzanie użytkownikami i grupami oraz uwierzytelnianie domenowe, b) możliwość równoczesnego użycia co najmniej 5 różnych baz LDAP, c) możliwość uruchomienia specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: i. SSL, ii. Radius, iii. Kerberos. d) możliwość transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy, e) co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta, f) autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny, g) rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie zdalnego pulpitu/aplikacji (VDI/RDS) stosowane w środowisku Zamawiającego (np. Citrix, RDS) lub rozwiązania równoważne, h) rozwiązanie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP), i) wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH, j) rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
3.5.11.	Administracja łączami do Internetu (ISP) & Routing a) rozwiązanie musi umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing), b) mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: i. równoważenie względem adresu źródłowego, ii. równoważenie względem połączenia. c) mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu, d) rozwiązanie musi umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover), e) rozwiązanie musi wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza, f) w zakresie SD-WAN rozwiązanie musi zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów), g) monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP, h) statyczne trasowanie pakietów, i) trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego, j) trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing),

	k) dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP, l) możliwość wybrania predefiniowalnego obiektu typu blackhole.
3.5.12.	Administracja a) konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego, b) interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS, c) administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. d) zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami, e) możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis, f) zarządzenie z poziomu konsoli (SSH), g) rozwiązanie musi umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania, h) Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS, i) wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup, j) wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, k) wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła, l) wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording), m) system musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services), n) portal uwierzytelniania (captive portal) dla użytkowników, o) eksport logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS), p) eksport logów za pomocą protokołu IPFIX, q) rozwiązanie musi umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: i. manualnego eksportu do pliku w dowolnym momencie czasu, ii. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu, r) odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora, s) anonimizacja logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika, t) rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego. u) wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu, v) system raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania, w) predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego,

	x) system raportowania ma umożliwiać eksport wyników raportu do formatu CSV, y) urządzenie musi umożliwiać przekazywanie logów do zewnętrznego systemu logowania/SIEM (np. syslog, API, CEF/LEEF lub równoważne), w tym możliwość dostarczenia przez wykonawcę komponentu pośredniczącego (np. VM/appliance) - bez ograniczenia co do producenta - o ile zapewnia pełną kompatybilność i wsparcie, z) możliwość monitorowania swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3, aa) możliwość monitorowania ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
3.5.13.	Pozostałe usługi i funkcje a) wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej, b) przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay), c) konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6, d) możliwość tworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny, e) rozwiązanie musi posiadać usługę DNS Proxy, f) wsparcie dla Spanning-tree protocol (RSTP/MSTP), g) wsparcie dla IEEE 802.1Q VLAN, h) zaimplementowane Open API, i) urządzenie musi posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie – lub inne rozwiązanie równoważne, j) urządzenie musi umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta, k) urządzenie nie ma limitu na liczbę użytkowników.
3.5.14.	Parametry sprzętowe: a) liczba portów Ethernet 2,5Gbps: min. 8 szt., b) liczba portów światłowodowych 1Gbps: min. 1, c) przepustowość Firewall (1518 bajtów UDP): min. 8 Gbps, d) przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP): min. 4 Gbps, e) przepustowość filtrowania Antywirusowego: min. 1 Gbps, f) przepustowość tunelu VPN przy szyfrowaniu AES: min. 2 Gbps, g) liczba tuneli VPN IPSec: min. 100, h) liczba tuneli typu SSL VPN (tryb tunelu): min. 100, i) obsługa interfejsów 802.11q (VLAN): min. 128, j) liczba równoczesnych sesji: min. 400.000 i nie mniej niż min. 20.000 nowych sesji/sekundę, k) urządzenie musi umożliwiać budowę klastra HA co najmniej w trybie Active–Passive, l) urządzenie musi posiadać moduł TPM.
3.5.15.	Ilość: 1 szt.
3.5.16.	System objęty serwisem gwarancyjnym producenta przez okres: min. zgodnie z pkt.2.3 na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
3.5.17.	Na potwierdzenie, że oferowane Urządzenie aktywne sieciowe spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć następujące dokumenty: a) opis proponowanego rozwiązania potwierdzający, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego urządzenia wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.
3.5.18.	W zakresie instalacji i konfiguracji urządzeń Wykonawca powinien zapewnić:

	a) ustalenie z Zamawiającym terminu przeprowadzenia prac, b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia, c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce), d) fizyczną instalację urządzeń aktywnych w szafach dystrybucyjnych 19", uwzględniającą podłączenie do zasilania 230V oraz wymaganego okablowania, e) konfigurację urządzenia zgodnie z wytycznymi Zamawiającego: i. rejestracja urządzenia / serwisów, ii. konfiguracja portu WAN, iii. konfiguracja portów LAN (do 5 podsieci), iv. konfiguracja VLAN (do 5 podsieci), v. konfiguracja Profili Bezpieczeństwa (1 per moduł), vi. konfiguracja Polityk Firewall (maks. 10 polityk), vii. konfiguracja przekierowań portów (do 5 portów), viii. konfiguracja VPN (Ipsec), ix. dodanie użytkowników (do 5 userów), x. konfiguracja monitorowania stanu urządzenia oraz tuneli VPN, xi. wdrożenie podstawowych reguł bezpieczeństwa z funkcjami antywirusowymi, IPS oraz filtrowaniem stron internetowych (3 polityki), xii. konfiguracja zewnętrznej komunikacji SYSLOG oraz SNMP dla monitorowania urządzenia, f) zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego.
3.5.19.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: a) dostawa: formalnemu odbiorowi podlega dostawa do Zamawiającego w ilościach określonych w pkt.3.5.15, b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzenia u Zamawiającego zgodnie z wykazem czynności określonym w pkt.3.5.18.

3.6. Urządzenie NAS (Network Attached Storage)*

3.6.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją urządzenia typu NAS (Network Attached Storage) na warunkach określonych w SWZ.
3.6.2.	Klasa produktu: NAS (Network Attached Storage).
3.6.3.	Procesor: min. czterordzeniowy min. 64-bitowy min. 3.3GHz.
3.6.4.	Obudowa: RACK 19" wraz z kompletem szyn umożliwiającym zamontowanie w szafie RACK.
3.6.5.	Pamięć RAM: zainstalowane min. 32GB DDR4 ECC, Uwaga: Pamięć RAM zgodna z listą kompatybilności producenta NAS. Zalecana konfiguracja instalacji: 2x 16GB RAM.
3.6.6.	Liczba zatok HDD: min. 12 szt.
3.6.7.	Obsługiwane dyski twarde (zakres minimalny): a) 3.5" SATA HDD / 2.5" SATA SSD – Hot Swap.
3.6.8.	Zainstalowane dyski twarde: a) min. 6 szt. 3.5" SATA HDD min. 20TB o parametrach nie gorszych niż: i. prędkość obrotowa: min. 7200 RPM, ii. MTTF: min. 2.500.000, iii. obciążenie roczne: min. 550 TB, iv. gwarancja producenta dysku: min. 24 mc-e,

	Uwaga: Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera. Dyski muszą być zgodne z listą kompatybilności producenta NAS.
3.6.9.	Porty na karty rozszerzeń: a) min. 1 szt. Gen3.
3.6.10.	LAN: a) min. 2 szt. 1GbE RJ-45, b) min. 1 szt. 10GbE RJ-45, c) min. 2 szt. 10GbE SFP+ Uwaga: W celu realizacji wymagania Zamawiający dopuszcza możliwość zastosowanie dodatkowych kart sieciowych z listy kompatybilności producenta NAS.
3.6.11.	Port USB: Tak (3.2).
3.6.12.	Redundantne zasilanie: a) zasilacz o mocy min. 350W.
3.6.13.	Obsługiwane tryby RAID: JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny.
3.6.14.	Pozostałe wymagania: a) Min. ilość dysków z opcjonalnymi modułami rozszerzającymi: min. 24 szt., b) mechanizm szyfrowania sprzętowego: Tak, c) uprawnienia: mechanizmy ACL dla udziałów SMB/CIFS (np. Windows ACL) lub równoważne.
3.6.15.	Usługa katalogowa: a) możliwość integracji z usługą katalogową LDAP/AD (np. Windows AD/Active Directory) lub równoważną Uwaga: Usługa musi umożliwiać użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station.
3.6.16.	Funkcje bezpieczeństwa: a) obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów): Tak, dla folderów współdzielonych i migawek, b) zapora sieciowa, c) szyfrowanie: i. folderu współdzielonego, ii. całego woluminu, iii. SMB, FTP (przez SSL/TLS), SFTP, d) automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów: i. HTTP, ii. HTTPS, iii. SMB, iv. SSH, v. Telnet, vi. FTP, e) obsługa Let's Encrypt, f) HTTPS (dostosowywane mechanizmy szyfrowania), g) dwuetapowa weryfikacja logowania (2FA) h) logowanie FIDO2/U2F lub inne rozwiązanie równoważne.
3.6.17.	Oprogramowanie do kopii zapasowej: a) b) kopia zapasowa całego systemu Windows (bare-metal) oraz przywracanie w trybie bare-metal, c) kopia zapasowa środowisk MacOS: Tak, pełna zgodność z plikami użytkownika,

	d) kopia zapasowa maszyn wirtualnych: środowiska wirtualizacji typu 1 wykorzystywane przez Zamawiającego (np. VMware, Hyper-V) lub równoważne, e) kopia zapasowa serwerów fizycznych: Windows, Linux, f) obsługa deduplikacji, kopii przyrostowych, kompresji oraz szyfrowania, g) obsługa wielu wersji i retencji dla plików kopii zapasowej, h) możliwość wyzwalania kopii zapasowej według harmonogramu (automatyzacja zadań), i) obsługa mechanizmów wysokiej dostępności (HA) dla środowisk wirtualizacji typu 1 wykorzystywanych przez Zamawiającego (np. klastry Hyper-V, VMware HA lub rozwiązania równoważne), j) automatyczna weryfikacja utworzonych kopii zapasowych poprzez symulowane odtworzenie (np. w formie wideo lub maszyny wirtualnej). k) centralne zarządzanie kopiami zapasowymi z jednej konsoli administracyjnej, l) konfiguracja nowych oraz edycja istniejących zadań backupowych dla wielu urządzeń (w tym harmonogramy, wersje i retencja), m) portal użytkownika do przywracania danych kopii zapasowej (bez konieczności posiadania uprawnień administratora), n) delegowanie uprawnień do zarządzania kopią zapasową oraz przywracaniem dla użytkowników z ograniczonymi uprawnieniami, o) kopia zapasowa usług chmur publicznych: Microsoft 365 oraz Google Workspace. Zgodność z oferowanym serwerem potwierdzona poprzez oficjalną dokumentację/listę kompatybilności (HCL) producenta oprogramowania lub producenta sprzętu, dopuszcza się równoważny dowód (np. oświadczenie Wykonawcy poparte dokumentacją producenta lub wynikami testu). Uwaga: Zgodność współpracy oprogramowania do kopii zapasowej z oferowanym NAS. Oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Jeżeli realizacja wymagania wymaga dostarczenia odrębnej(-ych) licencji to dostawa tych licencji stanowi Przedmiotu Zamówienia.
3.6.18.	Oprogramowanie: a) nowoczesny system plików zapewniający: i. obsługę migawek, ii. generowanie sum kontrolnych, iii. lustrzane kopie metadanych w celu zapewnienia integralności danych biznesowych, iv. ustawienie limitu dla folderów współdzielonych. v. szybkie klonowanie całych folderów udostępnionych, b) aplikacja do realizacji chmury prywatnej: i. konsola administratora zarządzaną z GUI, ii. agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS, iii. udostępnianie zasobów serwera NAS, iv. synchronizację i tworzenie kopii zapasowych podłączonych urządzeń, v. obsługa pracy z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny), vi. wsparcie dla wersjonowana oraz jednoczesnej edycję plików biurowych przez wielu użytkowników, Uwaga: Realizacja wymagania/funkcjonalności bez konieczności ponoszenia opłat abonamentowych (licencja wieczysta lub wbudowana funkcjonalność systemu NAS) c) klaster wysokiej dostępności (HA):

	i. możliwość stworzenia klastra HA z dwóch identycznych serwerów NAS, ii. automatyczne przełączanie dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego, d) kopia zapasowa danych serwera: i. tworzenie kopii zapasowej na zewnętrzne dyski twarde (USB), ii. kopia zapasowa do chmur publicznych, iii. kopia zapasowa na serwer rsync, e) obsługa migawek: i. min. 256 migawek na folder współdzielony, ii. min. 4000 migawek na cały system, f) funkcja serwera VPN: i. obsługa protokołów: OpenVPN, L2TP/IPSec, ii. wsparcie dla min. 10 jednoczesnych połączeń.
3.6.19.	Ilość: 2 szt.
3.6.20.	Gwarancja: a) gwarancji producenta serwera NAS b) okres: min. zgodnie z pkt.2.3.
3.6.21.	Gwarancja obejmuje: a) Gwarancja dotyczy również takich podzespołów sprzętowych takich jak pamięć RAM pkt.3.6.5, dyski twarde pkt. 3.6.8, karty sieciowe pkt. 3.6.10 oraz inne komponenty dostarczone w raz z serwerem NAS.
3.6.22.	Do czynności Wykonawcy w ramach montażu i uruchomienia serwera należy: a) ustalenie z Zamawiającym terminu przeprowadzenia prac, b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia, c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce), d) instalacja urządzenia zgodnie ze specyfikacjami produktu, w tym m.in. zamontowanie w szafach dystrybucyjnych, e) oznakowanie sprzętu naklejką, f) zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego.
3.6.23.	Na potwierdzenie, że oferowany Serwer backupu spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć do oferty następujące dokumenty: a) opis proponowanego rozwiązania potwierdzający, że oferowane urządzenie spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.
3.6.24.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: a) dostawa: formalnemu odbiorowi podlega dostawa w ilościach określonych w pkt.3.6.19, b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzeń zgodnie z wykazem czynności określonym w pkt.3.6.22.

3.7. Wsparcie ekspertów cyberbezpieczeństwa*

3.7.1.	Zakres przedmiotu zamówienia obejmuje zapewnienie przez Wykonawcę wsparcia dwóch ekspertów ds. cyberbezpieczeństwa, którzy będą pełnić funkcję pierwszej linii wsparcia technicznego podczas realizacji przedmiotu zamówienia opisanego w punktach 3.1 - 3.8. Eksperci ci mają wspierać działania Zamawiającego na każdym etapie wdrożenia dostarczanych systemów i usług, w szczególności w zakresie zapewnienia zgodności z wymaganiami bezpieczeństwa informacji, ciągłości działania oraz zgodności z obowiązującymi regulacjami.
3.7.2.	Wsparcie ekspertów ds. cyberbezpieczeństwa musi obejmować w szczególności:

	a) udział w analizie przedwdrożeniowej oraz opracowywaniu scenariuszy bezpieczeństwa wdrażanych rozwiązań, b) bieżące doradztwo w zakresie konfiguracji systemów z punktów 3.1 - 3.8 w sposób zapewniający zgodność z polityką bezpieczeństwa Zamawiającego, c) udział w pracach wdrożeniowych, w tym: i. wsparcie w konfiguracji istniejącej infrastruktury Zamawiającego w kontekście wdrożenia całości rozwiązań opisanych w SWZ, ii. weryfikacja poprawności konfiguracji i integracji komponentów z punktu widzenia bezpieczeństwa, iii. ocena ryzyk i propozycje mechanizmów ich ograniczania (w tym zgodność z OWASP, ISO/IEC 27001, KRI, NIS2), d) aktywne uczestnictwo w testach wdrożeniowych jako doradcy w zakresie zgodności testowanych funkcjonalności z wymaganiami bezpieczeństwa, e) doradztwo w zakresie utrzymania wdrożonego środowiska w zgodzie z najlepszymi praktykami (np. segmentacja sieci, kontrola dostępu, rejestrowanie i monitoring, zarządzanie incydentami), f) wsparcie w zakresie opracowania i/lub aktualizacji wewnętrznych procedur Zamawiającego związanych z eksploatacją wdrożonych rozwiązań w kontekście bezpieczeństwa informacji i infrastruktury krytycznej, g) identyfikację potencjalnych niezgodności, luk bezpieczeństwa lub słabych punktów w politykach i konfiguracjach, wraz z przygotowaniem rekomendacji, h) udział w spotkaniach projektowych oraz konsultacjach roboczych, i) analizę i korelację logów generowanych przez rozwiązania dostarczone przez Wykonawcę, w tym w szczególności przez systemy detekcji i zapobiegania włamaniom (IDS/IPS), systemy klasy SIEM oraz inne komponenty bezpieczeństwa objęte zakresem przedmiotu zamówienia, w celu identyfikacji incydentów, anomalii oraz prób naruszeń bezpieczeństwa. Analiza ta powinna być prowadzona z uwzględnieniem podejścia klasy SOAR (Security Orchestration, Automation and Response) i obejmować wsparcie dla Zamawiającego w zakresie opracowywania rekomendowanych scenariuszy reakcji oraz automatyzacji działań zaradczych, zgodnie z polityką bezpieczeństwa Zamawiającego.
3.7.3.	Wsparcie musi być świadczone w wymiarze łącznie 100 godzin, w tym: a) 80 godzin zdalnie (realizowanych przy użyciu zabezpieczonych kanałów komunikacji, np. VPN, zdalny pulpit, komunikatory szyfrowane), b) 20 godzin on-site, tj. stacjonarnie w lokalizacji Zamawiającego, w terminach uzgadnianych z odpowiednim wyprzedzeniem, Zamawiający dopuszcza możliwość, według własnego uznania, rozliczenia godzin wsparcia przewidzianych jako on-site w formule zdalnej, przy zachowaniu łącznego limitu 100 godzin wsparcia. Uwaga: Zamawiający ma prawo do wykorzystania wskazanego limitu godzin wsparcia najpóźniej do dnia określonego w pkt 2.3 OPZ.
3.7.4.	Wymaga się, aby: a) każdy z ekspertów posiadał minimum 3-letnie doświadczenie zawodowe w zakresie bezpieczeństwa systemów IT lub teleinformatycznych.
3.7.5.	Wykonawca jest zobowiązany do prowadzenia ewidencji przepracowanych godzin, rozliczanej godzinowo, z podziałem na tryb pracy zdalnej i on-site. Ewidencja musi być zatwierdzana przez Zamawiającego i stanowić podstawę rozliczenia wsparcia.
3.7.6.	Wsparcie ekspertów musi obejmować również: a) udział w min. dwóch spotkaniach projektowych (rozpoczęcie oraz zakończenie realizacji zamówienia),

	b) sporządzenie końcowego raportu eksperckiego z rekomendacjami dotyczącymi dalszego rozwoju i utrzymania bezpieczeństwa wdrożonych rozwiązań – dokument w języku polskim, w wersji edytowalnej i PDF.

3.8. Mechanizm bezpiecznego logowania*

3.1.20.	Zakres przedmiotu zamówienia obejmuje dostarczenie, instalację, konfigurację i uruchomienie mechanizmu bezpiecznego logowania, zapewniającego centralne zarządzanie tożsamościami i dostępem do systemów, integrującego się z istniejącym systemem dziedzinowym Zamawiającego oraz środowiskiem domenowym. Celem wdrożenia jest zwiększenie bezpieczeństwa poprzez kontrolę dostępu, eliminację wielokrotnego logowania oraz zabezpieczenie danych uwierzytelniających. Zamówienie obejmuje również udzielenie gwarancji jakości na okres: min. zgodnie z pkt.2.3. oraz świadczenie wsparcia technicznego, zgodnie z wymaganiami określonymi w niniejszej Specyfikacji.
3.1.21.	Wymaganie funkcjonalne: a) centralne zarządzanie kontami i uprawnieniami użytkowników, b) współpraca z kontrolerami domeny w środowisku Windows Server (np. Windows Server 2022) oraz systemami Linux (Debian ≥ 12), c) bezproblemowa integracja ze stacjami końcowymi wyposażonymi w systemy Windows w wersjach wspierających pracę w domenie (Professional lub Enterprise), d) możliwość integracji z systemem dziedzinowym w sposób umożliwiający tzw. pojedyncze logowanie (Single Sign-On), e) parametryzację i opcjonalność integracji z systemem dziedzinowym.
3.1.22.	Mechanizm bezpiecznego logowania musi spełniać następujące kryteria: a) wysoka dostępność i niezawodność działania, b) szyfrowanie całego procesu logowania (w tym transmisji danych), c) bezpieczne przechowywanie danych uwierzytelniających z wykorzystaniem silnych algorytmów kryptograficznych, d) możliwość definiowania polityk bezpieczeństwa (m.in. długość i złożoność hasła, wymuszenie zmiany hasła co określony czas), e) obsługa blokad po określonej liczbie nieudanych prób logowania (np. blokada konta na 5 minut po 3 nieudanych próbach), f) ograniczanie czasu trwania sesji oraz automatyczne kończenie sesji po wylogowaniu użytkownika, g) monitorowanie i rejestrowanie wszystkich prób logowania (zarówno udanych jak i nieudanych), h) wydajność zapewniająca szybkie logowanie bez opóźnień.
3.1.23.	Zakres integracji z systemem dziedzinowym a) autoryzacja użytkownika powinna następować automatycznie po uprzedniej autoryzacji użytkownika na stacji roboczej, b) mechanizm ma eliminować konieczność utrzymywania wielu kont w różnych systemach, c) możliwość skonfigurowania i uruchomienia integracji jako opcji konfiguracyjnej.
3.1.24.	Ilość: 1 komplet.
3.1.25.	Wykonawca zapewni: a) przeprowadzenie aktualizacji systemu dziedzinowego w zakresie niezbędnym do działania mechanizmu, b) wsparcie przy konfiguracji i mapowaniu kont użytkowników między systemem dziedzinowym a kontrolerem domeny, c) instruktaż i asystę stanowiskową dla administratora systemu, d) dostarczanie aktualizacji dokumentacji użytkownika każdorazowo wraz z nową wersją mechanizmu lub systemu dziedzinowego,

	e) świadczenie usług wsparcia technicznego i utrzymaniowego przez okres wskazany w pkt 3.6.7, w zakresie zapewniającym nieprzerwane i bezpieczne funkcjonowanie wdrożonego mechanizmu.
3.1.26.	Gwarancja: min. zgodnie z pkt.2.3. na dostarczony mechanizm oraz świadczone wsparcie techniczne. Uwaga: Wykonawca udzieli gwarancji jakości na okres min. zgodnie z pkt.2.3. na dostarczony mechanizm oraz będzie świadczył wsparcie techniczne i serwisowe przez okres co najmniej 12 miesięcy od dnia podpisania protokołu odbioru. Wsparcie obejmuje w szczególności rozwiązywanie problemów technicznych, dostarczanie aktualizacji, konsultacje konfiguracyjne oraz pomoc w bieżącym utrzymaniu rozwiązania.” Wsparcie techniczne.
3.1.27.	Do czynności Wykonawcy w ramach instalacji, konfiguracji i uruchomienie mechanizmu bezpiecznego logowania należy: h) ustalenie z Zamawiającym terminu przeprowadzenia prac, i) przygotowanie środowiska systemowego i sieciowego do wdrożenia mechanizmu (w tym kontroler domeny), j) instalacja i konfiguracja komponentów mechanizmu na serwerze lub wskazanym środowisku, k) integracja mechanizmu z systemem dziedzinowym oraz kontrolerem domeny, l) mapowanie kont użytkowników pomiędzy domeną a systemem dziedzinowym, m) konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami Zamawiającego (np. złożoność hasła, blokady, czas sesji), n) testy funkcjonalne mechanizmu logowania, w tym testy poprawności konfiguracji, o) weryfikacja zgodności z wymaganiami niefunkcjonalnymi (szyfrowanie, bezpieczeństwo sesji, rejestrowanie prób logowania), p) przekazanie raportu z wdrożenia zawierającego m.in. dokumentację konfiguracyjną oraz potwierdzenie poprawnego działania, q) odbiór techniczny wraz z podpisaniem protokołu wdrożenia.
3.1.28.	Na potwierdzenie, że oferowany mechanizm bezpiecznego logowania (SSO) spełnia wymagania określone przez Zamawiającego, Wykonawca zobowiązany jest dołączyć do oferty następujące dokumenty: a) opis proponowanego rozwiązania, potwierdzający, że oferowany mechanizm bezpiecznego logowania spełnia wszystkie wymagania funkcjonalne i niefunkcjonalne określone w SWZ. Opis powinien zawierać: a) nazwę producenta, b) typ i wersję oferowanego rozwiązania, c) rodzaj oraz warunki licencji, d) szczegółowy wykaz wszystkich komponentów składających się na system, e) informację o możliwości integracji z systemem dziedzinowym oraz środowiskami Windows Server i Linux, f) informacje o mechanizmach bezpieczeństwa, szyfrowaniu danych, zarządzaniu sesjami i politykach haseł (jeżeli dotyczy), g) wykaz elementów objętych dostawą i wdrożeniem.
3.1.29.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: c) dostawa: formalnemu odbiorowi podlega dostawa mechanizmu bezpiecznego logowania wraz ze wszystkimi komponentami niezbędnymi do jego uruchomienia, zgodnie z zakresem określonym w pkt 3.8.5, d) Instalacja i konfiguracja: formalnemu odbiorowi podlega wykonanie czynności instalacyjnych, konfiguracyjnych i wdrożeniowych, zgodnie z zakresem wskazanym

	w pkt 3.6.8, w tym instalacja, konfiguracja, testy poprawności działania, weryfikacja zgodności z wymaganiami oraz integracja z systemem dziedzinowym i środowiskiem domenowym Zamawiającego.

3.9. Oprogramowanie Systemowe typ I (SSO)

3.9.1.	Oprogramowanie Systemowe typ I - Serwerowy System Operacyjny (SSO).
3.9.2.	Oprogramowanie systemowe typ I (SSO) musi spełniać wymagania minimalne opisane w pkt. od 3.9. oraz pochodzić z najnowszej linii produktowej Producenta oraz musi być dostarczone w najnowszej dostępnej produkcyjnie (GA) wersji na dzień składania oferty.
3.9.3.	Licencja na SSO musi uprawniać do zainstalowania SSO w środowisku fizycznym oraz umożliwiać zainstalowanie nielimitowanej ilości instancji wirtualnych tego SSO. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze, oraz dostarczona w najnowszej dostępnej wersji. Uwaga: Licencja SSO musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze opisanym w pkt.3.1 oraz pkt.3.2.
3.9.4.	Licencja dożywotnia nie może być ograniczona czasowo.
3.9.5.	Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. a) możliwość wykorzystania min. 320 logicznych procesorów oraz co najmniej min. 4TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania min. 64 procesorów wirtualnych oraz min. 1TB pamięci RAM i dysku o pojemności do 64TB min. przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z min. 64 węzłów, z możliwością uruchamiania min. 7000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading) i) wbudowane wsparcie instalacji i pracy na wolumenach, które: i. pozwalają na zmianę rozmiaru w czasie pracy systemu, ii. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, iii. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, iv. umożliwiają zdefiniowanie list kontroli dostępu (ACL),

	j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. l) możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
3.9.6.	Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
3.9.7.	Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
3.9.8.	Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
3.9.9.	Pozostałe wymagania: a) mechanizmy logowania w oparciu o: i. Login i hasło, ii. Karty z certyfikatami (smartcard), iii. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), b) możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: i. określonych grup użytkowników, ii. zastosowanej klasyfikacji danych, iii. centralnych polityk dostępu w sieci, iv. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych, v. bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o systemy iOS oraz Windows 8.1, c) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), d) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, e) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, f) pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management), g) wsparcie dla środowisk Java i .NET Framework 4.x (możliwość uruchomienia aplikacji działających we wskazanych środowiskach).
3.9.10.	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. 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 pozwalające na uruchamianie do min. 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. możliwość wirtualizacji sieci z zastosowaniem przełącznika wirtualnego, którego funkcjonalność może być rozszerzana równolegle poprzez oprogramowanie kilku różnych dostawców za pomocą otwartego interfejsu API, vi. możliwość kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. tryb trunk), n) 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, o) wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath), p) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, q) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, r) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.