

Nr sprawy: RIZP.271.6.2025.DO.

Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Wstęp	2
2. Wymagania ogólne.....	4
3. Opis przedmiotu zamówienia	5
3.1 Zadanie 1: Serwer kopii wraz z dyskami i oprogramowaniem	5
3.2 Zadanie 2: Oprogramowanie do wykonywania kopii wraz z wdrożeniem	13
3.3 Zadanie 3: UPS stanowiskowe – 10 szt.	29
3.4 Zadanie 4: Zakup dodatkowego urządzenia klasy UTM plus licencje dla 2 urządzeń	31
3.5 Zadanie 5: Wielofunkcyjne źródło zasilania	39
3.6 Zadanie 6: Przełączniki sieciowe.....	40
Przełącznik 24 portowy – 1 sztuka	40
Przełączniki 16 portowe – 2 szt.	41
Przełączniki 8 portowe – 3 szt.....	42
3.7 Zadanie 7: Zakup serwera fizycznego oraz systemu Windows Server lub równoważnego wraz z wdrożeniem i konfiguracją	43
3.8 Zadanie 8: Zlecenie instalacji, konfiguracji i wsparcia technicznego oprogramowania OpenSource do zarządzania logami	51
3.9 Zadanie 9: Zakup serwera na potrzeby oprogramowania do zarządzania logami oraz do zarządzania infrastrukturą IT wraz z niezbędnym oprogramowaniem systemowym	54
3.10 Zadanie 10: Zakup oprogramowania do zarządzania infrastrukturą IT wraz z usługą instalacji i konfiguracji	57
3.11 Zadanie 11: Zakup szkolenia dla pracowników obsługi informatycznej z obsługi i użytkowania oprogramowania do analizy logów systemowych	59
3.12 Zadanie 12: Zakup szkolenia dla pracowników obsługi informatycznej z obsługi i użytkowania oprogramowania do zarządzania infrastrukturą	61
3.13 Zadanie 13: Zakup szkolenia dla pracowników wydziału informatyki z technologii Windows Server	62

1. Wstęp

1.1. Cel zamówienia

Celem zamówienia jest poprawa bezpieczeństwa i niezawodności infrastruktury IT Urzędu Miejskiego w Białym Borze poprzez wdrożenie systemu backupu, zakup i konfigurację sprzętu oraz wdrożenie oprogramowania do zarządzania logami i infrastrukturą IT. Systemy te mają na celu zapewnienie ochrony przed utratą danych, zwiększenie odporności na awarie oraz optymalizację zarządzania zasobami informatycznymi. Dodatkowo, zakup szkoleń dla pracowników ma na celu zapewnienie prawidłowej eksploatacji wdrożonych rozwiązań.

1.2. Zakres przedmiotu zamówienia

Przedmiot zamówienia obejmuje dostawę, instalację, konfigurację i wdrożenie następujących elementów infrastruktury IT:

1. **System backupu:** zakup serwera do przechowywania kopii zapasowych, oprogramowania backupowego oraz jego wdrożenie i konfiguracja. System umożliwi wykonywanie kopii zapasowych baz danych, środowisk wirtualnych oraz profili użytkowników.
2. **Urządzenia UTM:** zakup i wdrożenie urządzeń do zarządzania ruchem sieciowym i ochrony przed cyberzagrożeniami.
3. **Zasilanie awaryjne:** zakup UPS-ów stanowiskowych oraz wielofunkcyjnego źródła zasilania awaryjnego w celu zapewnienia ciągłości pracy infrastruktury IT.
4. **Przełączniki sieciowe:** modernizacja infrastruktury sieciowej poprzez zakup nowych przełączników.
5. **Serwer fizyczny z systemem Windows Server (lub równoważny):** zakup i konfiguracja serwera na potrzeby centralnego zarządzania infrastrukturą IT oraz realizacji polityki backupu.
6. **System do zarządzania logami:** zakup serwera oraz wdrożenie oprogramowania OpenSource do centralnego zbierania i analizy logów systemowych.

7. **Szkolenia:** realizacja szkoleń dla pracowników IT w zakresie obsługi oprogramowania do analizy logów, zarządzania infrastrukturą IT oraz technologii Windows Server.

1.3. Podział zamówienia na zadania

Zamówienie podzielone jest na następujące zadania:

Zadanie 1: Dostawa serwera kopii zapasowych wraz z dyskami i oprogramowaniem.

Zadanie 2: Dostawa oprogramowania do backupu wraz z wdrożeniem i konfiguracją.

Zadanie 3: Dostawa 10 sztuk UPS-ów stanowiskowych.

Zadanie 4: Zakup dodatkowego urządzenia UTM oraz licencji dla dwóch urządzeń.

Zadanie 5: Zakup wielofunkcyjnego źródła zasilania awaryjnego.

Zadanie 6: Zakup przełączników sieciowych.

Zadanie 7: Zakup serwera fizycznego wraz z systemem Windows Server lub równoważnym, jego wdrożenie i konfiguracja.

Zadanie 8: Instalacja, konfiguracja i wsparcie techniczne oprogramowania OpenSource do zarządzania logami.

Zadanie 9: Zakup serwera na potrzeby oprogramowania do zarządzania logami oraz infrastrukturą IT.

Zadanie 10: Zakup oprogramowania do zarządzania infrastrukturą IT wraz z usługą instalacji i konfiguracji.

Zadanie 11: Szkolenie dla pracowników IT w zakresie obsługi oprogramowania do analizy logów systemowych.

Zadanie 12: Szkolenie dla pracowników IT w zakresie zarządzania infrastrukturą IT.

Zadanie 13: Szkolenie dla pracowników wydziału informatyki z technologii Windows Server.

2. Wymagania ogólne

2.1. Warunki realizacji zamówienia

Miejsce realizacji: dostawa, instalacja oraz konfiguracja sprzętu i oprogramowania objętego zamówieniem odbędzie się w **siedzibie Urzędu Miejskiego w Białym Borze, ul. Słupska 10, 78-425 Biały Bór.**

Godziny realizacji prac: wszelkie prace instalacyjne, konfiguracyjne oraz szkoleniowe muszą być realizowane w godzinach pracy urzędu, tj.:

- **poniedziałek:** 07:15–16:30
- **wtorek – czwartek:** 07:15–15:15
- **piątek:** 07:15–14:00

Wykonawca jest zobowiązany do wcześniejszego uzgodnienia terminu dostawy oraz harmonogramu wdrożenia z Zamawiającym.

Koszt dostawy: wszelkie koszty związane z dostawą, transportem oraz wniesieniem sprzętu leżą po stronie Wykonawcy.

Instalacja i konfiguracja: Wykonawca zobowiązany jest do dostarczenia, zainstalowania oraz skonfigurowania dostarczonego sprzętu i oprogramowania zgodnie z niniejszym opisem przedmiotu zamówienia.

2.2. Wymagania dotyczące dokumentacji technicznej i odbioru

Dokumentacja techniczna

Wykonawca jest zobowiązany dostarczyć pełną dokumentację techniczną dla każdego dostarczonego elementu sprzętowego i oprogramowania, w tym:

- **Dokumentację instalacyjną i konfiguracyjną** – opisującą szczegółowe instrukcje dotyczące instalacji i konfiguracji sprzętu oraz oprogramowania.
- **Instrukcję obsługi** – zawierającą zasady użytkowania i zarządzania wdrożonym systemem, dedykowaną dla administratorów oraz użytkowników.
- **Dokumentację powdrożeniową** – podsumowującą zrealizowane wdrożenie, opisującą sposób integracji systemów oraz wszelkie modyfikacje konfiguracji wprowadzone podczas instalacji.
- **Dokumentację licencyjną** – w przypadku dostarczenia oprogramowania Wykonawca dostarczy oryginalne licencje oraz warunki użytkowania oprogramowania.

Procedura odbioru

- Odbiór dostarczonego sprzętu i oprogramowania zostanie przeprowadzony przez zamawiającego po zakończeniu instalacji, konfiguracji oraz wykonaniu testów poprawności działania.
- Wykonawca zobowiązany jest przeprowadzić testy wdrożeniowe w obecności przedstawicieli zamawiającego w celu potwierdzenia zgodności wdrożenia z wymaganiami określonymi w zamówieniu.
- Po pomyślnym zakończeniu testów Wykonawca przedstawi protokół odbioru końcowego, który musi zostać podpisany przez obie strony.
- W przypadku stwierdzenia usterek lub niezgodności, wykonawca zobowiązany jest do ich nieodpłatnego usunięcia w uzgodnionym terminie.

Wymagania dotyczące gwarancji i serwisu

- Sprzęt i oprogramowanie muszą być objęte gwarancją zgodnie z warunkami określonymi w specyfikacji zamówienia.
- Wykonawca zapewni wsparcie techniczne w zakresie obsługi i eksploatacji dostarczonych rozwiązań zgodnie z umową.
- Szczegółowe warunki gwarancji i serwisu, w tym czasy reakcji i napraw, określono w opisie poszczególnych zadań.
- Wszelkie zgłoszenia serwisowe i reklamacje będą obsługiwane przez Wykonawcę w ustalonym w umowie czasie reakcji.

3. Opis przedmiotu zamówienia

3.1 Zadanie 1: Serwer kopii wraz z dyskami i oprogramowaniem

L.p.	Wymaganie	Opis wymagania
1	Cel	<p>Celem zamówienia jest zapewnienie bezpiecznego i efektywnego systemu do przechowywania oraz zarządzania kopiami zapasowymi danych w Urzędzie Miejskim w Białym Borze.</p> <p>Zakupiony serwer backupu będzie zabezpieczał kopie baz danych systemów dziedzinowych, profile użytkowników oraz środowiska wirtualne.</p> <p>System musi być zintegrowany z infrastrukturą IT urzędu.</p>

		<p>Będzie wykorzystywane do backupu:</p> <ol style="list-style-type: none"> 1. baz danych systemów dziedzinowych, w tym: <ul style="list-style-type: none"> • Microsoft SQL, PostgreSQL, Firebird 1. profili użytkowników przechowywanych na serwerze opisanym w zadaniu 7 oraz kopii danych z komputerów użytkowników końcowych . 2. środowisk wirtualnych, które powstaną w ramach niniejszego zamówienia i zostaną stworzone przez wykonawcę. 3. Kopii plikowych związanych z oprogramowaniem.
2	Procesor	<p>Przeznaczenie do zastosowań w urządzeniach działających 24/7, takich jak: serwery NAS, systemy backupu.</p> <p>Minimum 4 rdzenie fizyczne,</p> <p>Minimum 8 wątków logicznych,</p> <p>Taktowanie bazowe min. 2.2 GHz</p>
3	Pamięć RAM	Minimum 8 GB z możliwością rozbudowy do co najmniej 32 GB
4	Liczba zatok na dyski	Minimum 8 zatok na dyski 3.5" lub 2.5".
5	Obsługa Hot-Swap	Tak
6	Porty USB	Minimum 2 porty USB 3.2 Gen 1
7	Porty sieciowe	Minimum 2 x 1GbE RJ-45 oraz minimum 1 x 10GbE
8	Obsługa RAID	Obsługa RAID 0, 1, 5, 6, 10
9	Obsługa wirtualizacji	Obsługa VMware, Microsoft Hyper-V
10	Obsługa SSD Cache	Wsparcie dla SSD cache
11	Protokoły sieciowe	Obsługa SMB, NFS, FTP, WebDAV
12	Wymiary	Urządzenie musi być przystosowane do montażu w standardowej szafie rack 19" oraz mieć maksymalną wysokość 3U. Wykonawca musi dostarczyć wszystkie niezbędne elementy montażowe, takie jak prowadnice, szyny montażowe oraz śruby.
13	Chłodzenie	Wentylatory redundantne (hot-swap).
14	Zakres temperatury	Od 10°C do 35°C

	pracy	
15	Zasilanie	Redundantny zasilacz, przystosowany do zasilania napięciem zgodnym z polskimi standardami dostarczania energii elektrycznej, tj. 230 V przy częstotliwości 50 Hz. Zasilacze muszą mieć możliwość zasilenia serwera poprzez wielofunkcyjne źródło zasilania opisane w Zadaniu 5.
16	Maksymalna możliwa rozbudowa pojemności dyskowej	Urządzenie musi umożliwiać rozbudowę przestrzeni dyskowej do co najmniej 64 TB poprzez dodanie kolejnych dysków w dostępnych zatokach.
17	Wymagane dyski	<p>Zamawiający wymaga dostarczenia minimum 6 (sześciu) dysków twardych o pojemności 16 TB każdy, kompatybilnych z oferowanym serwerem. Dyski muszą być klasy enterprise/NAS, przeznaczone do pracy 24/7.</p> <p>Konfiguracja RAID 10 musi zapewniać nie mniej niż 48 TB efektywnej pojemności użytkowej.</p> <p>Urządzenie musi jednocześnie umożliwiać dalszą rozbudowę przestrzeni dyskowej tak, aby docelowo osiągnąć co najmniej 64 TB efektywnej pojemności.</p>
18	Wsparcie dla mechanizmów backupów i snapshot	Serwer musi być kompatybilny i współpracować z mechanizmami backupów, snapshotów opisanych w tabeli "Oprogramowanie do wykonywania kopii wraz z wdrożeniem" - Zadanie 2.
19	Oprogramowanie zarządzające	Musi posiadać wbudowany interfejs zarządzania dostępny np. przez przeglądarkę oraz CLI.
20	Wymagana zgodność z istniejącym środowiskiem kopii zapasowych	<p>Urząd Miejski w Białym Borze obecnie wykorzystuje serwer kopii zapasowych Synology RS1221RP+ jako lokalne repozytorium backupu danych.</p> <p>Zamawiający wymaga, aby oferowane rozwiązanie (serwer kopii zapasowych wraz z oprogramowaniem i dyskami) umożliwiała współpracę z istniejącym serwerem Synology RS1221RP+ w zakresie realizacji zdalnych kopii zapasowych. Współpraca ta musi obejmować możliwość przesyłania kopii danych z serwera Synology RS1221RP+ do nowego urządzenia.</p>

		<p>Oferowane rozwiązanie musi umożliwiać obsługę protokołów i metod przesyłania danych kompatybilnych z RS1221RP+.</p> <p>Wykonawca zobowiązany jest do wdrożenia oferowanego rozwiązania, obejmującego w szczególności:</p> <ul style="list-style-type: none"> • instalację i konfigurację urządzenia w siedzibie Urzędu Miejskiego w Białym Borze. • integrację z obecnym serwerem Synology RS1221RP+, • skonfigurowanie mechanizmów zdalnego backupu zgodnie z wymaganiami Zamawiającego, • przetestowanie poprawności przesyłu i odtwarzania kopii zapasowych.
21	Dokumentacja urządzenia	<p>Wykonawca musi dostarczyć pełną dokumentację urządzenia (w wersji papierowej lub elektronicznej), w tym:</p> <ol style="list-style-type: none"> a. Instrukcję instalacji, b. Instrukcję użytkownika, c. Dokumentację techniczną zawierającą opis funkcjonalności sprzętu i oprogramowania, d. Opis konfiguracji sieciowej (porty, protokoły itp.), e. Dokumentacja musi być dostarczona w języku polskim lub w języku angielskim. f. Wykonawca musi zapewnić dostęp do bieżących aktualizacji dokumentacji i instrukcji (np. w postaci plików PDF na stronie producenta lub nośniku elektronicznym) przez cały okres gwarancji. g. W przypadku zmian lub aktualizacji oprogramowania (firmware), wykonawca zobowiązuje się dostarczyć zamawiającemu zaktualizowane instrukcje lub wskazać oficjalne źródło pobrania takiej dokumentacji.
22	Wymagana gwarancja	<ol style="list-style-type: none"> 1. Dostarczony serwer musi być objęty

		<p>gwarancją przez okres 36 miesięcy, liczony od daty podpisania protokołu odbioru końcowego.</p> <p>2. W ramach gwarancji Wykonawca zapewnia serwis w siedzibie zamawiającego, obejmujący naprawę lub wymianę urządzenia na sprawne. Maksymalny czas na usunięcie awarii wynosi 24 godziny, liczone od momentu zgłoszenia awarii przez Zamawiającego.</p> <p>3. Zgłoszenie awarii może nastąpić poprzez:</p> <ul style="list-style-type: none">a. e-mail wysłany na adres serwisowy wskazany przez Wykonawcę,b. aplikację/webowy portal serwisowy udostępniony przez Wykonawcę. <p>4. Potwierdzenie przyjęcia zgłoszenia przez Wykonawcę musi nastąpić nie później niż w ciągu 4 godzin od chwili otrzymania zgłoszenia (e-mailem lub w aplikacji). W ramach potwierdzenia Wykonawca przekazuje Zamawiającemu:</p> <ul style="list-style-type: none">a. datę i godzinę przyjęcia zgłoszenia,b. unikalny identyfikator zgłoszenia pozwalający na śledzenie postępu,c. przewidywany termin zakończenia naprawy. <p>5. Jeżeli Wykonawca nie potwierdzi przyjęcia zgłoszenia w ww. terminie 4 godzin, wówczas 24-godzinny czas na usunięcie awarii liczony jest od momentu wysłania zgłoszenia awarii przez Zamawiającego (tj. data i godzina wysłania e-maila lub odnotowania zgłoszenia w aplikacji/portalu).</p> <p>6. W przypadku uszkodzenia dysków twardych, Zamawiający wymaga pozostawienia ich w swojej siedzibie (dyski nie podlegają zwrotowi do Wykonawcy).</p>
--	--	--

		<p>7. Cała komunikacja z zespołem serwisowym (w tym zgłaszanie awarii, potwierdzenia, informacje o statusie naprawy) odbywa się w języku polskim, ze względu na konieczność zapewnienia ciągłości obsługi technicznej przez polskojęzyczny personel urzędu.</p> <p>W ramach gwarancji producent lub dostawca sprzętu musi zapewnić:</p> <p>1. Dostęp do najnowszych aktualizacji oprogramowania, związanego ze sprzętem, które mają na celu utrzymanie oprogramowania w pełni funkcjonalnym, muszą obejmować poprawki bezpieczeństwa, aktualizacje kompatybilności z dostarczonymi systemami operacyjnymi oraz dostarczonym oprogramowaniem do backupu, jak również wszelkie usprawnienia funkcjonalne i optymalizacyjne dostarczane przez producenta oprogramowania mające na celu zapewnienie bezpieczeństwa oprogramowania, w przypadku ujawnienia podatności bezpieczeństwa (np. CVE) w dostarczonym oprogramowaniu związanym ze sprzętem, celem usunięcia tych podatności i uzyskania oprogramowania wolnego od podatności bezpieczeństwa.</p> <p>2. Wszystkie aktualizacje muszą być dostarczane bez dodatkowych kosztów dla Zamawiającego, a procedury ich wdrażania muszą być jasno opisane w dokumentacji technicznej.</p>
23	Wdrożenie	<p>1. Analiza przedwdrożeniowa</p> <p>a. Weryfikacja środowiska Zamawiającego poprzez ustalenie szczegółowej konfiguracji posiadanych serwerów, systemów dziedzinowych, infrastruktury sieciowej.</p> <p>b. Określenie szczegółowych wymagań w odniesieniu do harmonogramu wykonywania kopii zapasowych, retencji (przechowywania historycznych wersji)</p>

		<p>c. Doprecyzowanie zapotrzebowania na przepustowość sieci, ewentualnych wymagań co do segmentacji sieci lub przydziału adresów IP.</p> <p>2. Dostawa i instalacja sprzętu</p> <p>a. Dostawa serwera backupu i dysków.</p> <p>b. Umieszczenie urządzenia w docelowej szafie rack 19" (w siedzibie Urzędu) oraz fizyczne podłączenie do infrastruktury zasilania.</p> <p>c. Konfiguracja interfejsów sieciowych urządzenia w sposób zapewniający wymaganą komunikację z istniejącymi serwerami i segmentami sieciowymi.</p> <p>3. Konfiguracja systemu operacyjnego i oprogramowania serwera backupu</p> <p>a. Utworzenie i konfiguracja RAID, aby zapewnić wymaganą pojemność i poziom bezpieczeństwa danych.</p> <p>b. Instalacja i wstępna konfiguracja oprogramowania do zarządzania kopiami zapasowymi, w tym ustawienie parametrów bezpieczeństwa (kont użytkowników, protokołów szyfrowania, uprawnień).</p> <p>c. Integracja z oprogramowaniem systemowym i wirtualizacyjnym.</p> <p>4. Integracja z obecnym serwerem Synology RS1221RP+</p> <p>a. Skonfigurowanie reguł przesyłu danych z Synology RS1221RP+ do nowego urządzenia .</p> <p>5. Konfiguracja i testy mechanizmów zdalnego backupu</p> <p>a. Zaplanowanie, które zasoby (bazy danych, pliki, profile użytkowników, systemy wirtualne, itp.) mają być archiwizowane do lokalizacji zewnętrznej i w jakich przedziałach czasowych.</p> <p>b. Sprawdzenie i optymalizacja konfiguracji sieci pod kątem transferu dużych ilości danych poza główną siedzibę.</p> <p>c. Przeprowadzenie próbnych backupów i odtworzeń w celu potwierdzenia szybkości transferu i prawidłowego działania</p>
--	--	---

procedur w razie awarii.

6. Wdrożenie kopii z komputerów użytkowników końcowych

- a. Instalacja/konfiguracja agentów backupu (lub odpowiednich klientów) na stacjach roboczych, jeśli zamawiający wymaga kopiowania danych bezpośrednio z komputerów użytkowników.
- b. Optymalizacja polityk kopiowania (np. wykluczenia pewnych folderów, ustalenie harmonogramu kopiowania poza godzinami pracy urzędu).
- c. Wykonanie próbnego przywrócenia plików lub profili użytkownika w celu weryfikacji, że kopie z komputerów końcowych są poprawne.

7. Instruktaż i dokumentacja powdrożeniowa

- a. Przeprowadzenie instruktażu dla osób wyznaczonych przez Zamawiającego w zakresie obsługi nowego urządzenia (logowanie, podstawowe operacje backupu/restore, monitorowanie stanu systemu).
- b. Przekazanie dokumentacji -komplet instrukcji w języku polskim lub angielskim (w formie papierowej lub elektronicznej), obejmujących m.in.
 - szczegółową konfigurację macierzy RAID i sieci,
 - opis harmonogramów i polityk backupu,
 - procedury przywracania danych,
 - procedury zgłaszania usterek w ramach gwarancji.

8. Testy końcowe i odbiór rozwiązania

- a. Przeprowadzenie kompleksowych testów w obecności przedstawiciela Zamawiającego - sprawdzenie, czy urządzenie i oprogramowanie działają zgodnie z założeniami, a dane można przywrócić z kopii w razie potrzeby.

3.2 Zadanie 2: Oprogramowanie do wykonywania kopii wraz z wdrożeniem

L.p.	Wymaganie	Opis wymagania
1	Cel	<p>Celem zamówienia jest nabycie licencji oraz wdrożenie systemu backupu danych dla Urzędu Miejskiego w Białym Borze, który zapewni skuteczną ochronę, przechowywanie oraz odzyskiwanie danych w przypadku awarii lub utraty danych. System backupu ma służyć wyłącznie na potrzeby wewnętrzne urzędu i być administrowany przez jego pracowników.</p> <p>Oprogramowanie backupu musi również umożliwiać wykonywanie kopii zapasowych z komputerów użytkowników końcowych (stacji roboczych). Dopuszcza się w tym celu zastosowanie agentów instalowanych na komputerach lub innych mechanizmów oferowanych przez oprogramowanie backupu</p>
2	Licencja	<p>Licencje na system backupu, muszą umożliwiać:</p> <ul style="list-style-type: none"> wykorzystanie systemu wyłącznie na potrzeby wewnętrzne zamawiającego. System będzie administrowany i eksploatowany bezpośrednio przez pracownika zamawiającego prawo do instalacji, konfiguracji, użytkowania oraz zarządzania systemem backupu. <p>Zamawiający uzyska uprawnienia do korzystania z oprogramowania do backupu wraz z momentem podpisania protokołu odbioru końcowego, który nastąpi po pomyślnym zainstalowaniu i przetestowaniu systemu zgodnie z określonymi w niniejszej tabeli – wiersz 35. Odbiór końcowy oprogramowania stanowi moment, od którego zamawiający może w pełni korzystać z systemu backupu w ramach swojej organizacji.</p> <p>Zamawiający dopuszcza następujące formy licencjonowania oprogramowania do</p>

backupu:

1. Licencjonowanie wg. ilości maszyn wirtualnych (VM): oprogramowanie do backupu ma być licencjonowane na podstawie liczby maszyn wirtualnych, które będą chronione przez to oprogramowanie.
2. Licencjonowanie wg. Ilości serwerów fizycznych: oprogramowanie do backupu ma być licencjonowane na podstawie ilości serwerów fizycznych, które będą chronione przez to oprogramowanie. Licencje mogą być przyznawane na każdy serwer fizyczny oddzielnie.
3. Licencjonowanie wg. ilości danych (per TB): oprogramowanie do backupu ma być licencjonowane na podstawie ilości danych przechowywanych w systemie backupu. Licencje mają być określane na podstawie całkowitej pojemności danych w terabajtach (TB). Przy licencjonowaniu wg. ilości danych nie może być ograniczeń co do liczby chronionych maszyn wirtualnych. Licencja musi obejmować niezduplowane i nieskompresowane dane źródłowe.
4. Licencjonowanie bez ograniczeń: model licencji ma pozwalać na nieograniczone wykorzystanie oprogramowania bez limitów co do liczby maszyn wirtualnych, liczby procesorów (socketów), oraz ilości danych przechowywanych w systemie backupu. Model ten musi umożliwiać elastyczne dostosowanie zasobów backupowych do aktualnych i przyszłych potrzeb zamawiającego. Licencja w modelu bez ograniczeń musi obejmować również prawo do wykonania backupu i odtwarzania danych z dowolnych źródeł, w tym z maszyn wirtualnych, baz danych i plików, niezależnie od ich wielkości i lokalizacji.
5. Licencjonowanie na podstawie liczby gniazd procesora fizycznego (zajętych socketów) na chronionych hostach. Licencja musi

		<p>umożliwiać backup/odtworzenie:</p> <ul style="list-style-type: none"> - dowolnej liczby maszyn wirtualnych jako obrazów, - agentowo: dowolnej liczby baz danych, plików, ze środka maszyn wirtualnych, - dowolnej liczby TB w zabezpieczanym środowisku. <p>6. Zamawiający dopuszcza również możliwość wykorzystania oprogramowania backupowego typu open source, które może być używane bez tradycyjnych opłat licencyjnych. Oprogramowanie open source musi zapewniać wszystkie funkcje wskazane w wierszach tabeli od 1– do 35.</p> <p>Typ licencji oprogramowania do backupu:</p> <ol style="list-style-type: none"> 1. Licencja wieczysta: Licencja wieczysta musi uprawniać do nieograniczonego czasowo użytkowania oprogramowania. W ramach licencji wieczystej, zamawiający musi otrzymać pełny dostęp do funkcjonalności oprogramowania oraz prawo do korzystania z oprogramowania na stałe. 2. Licencja typu open source: Oprogramowanie backupowe może być również dostępne na licencji open source, co umożliwia użytkowanie bez dodatkowych opłat licencyjnych. <p>W ramach licencji Urząd Miejski w Białym Borze, uzyska nieograniczone, wieczyste prawo do korzystania z systemu backupu. System będzie wykorzystywany wyłącznie na potrzeby wewnętrzne Urzędu, administrowany i eksploatowany bezpośrednio przez pracowników Urzędu Miejskiego w Białym Borze. Prawo do korzystania obejmuje instalację, konfigurację, użytkowanie oraz zarządzanie systemem backupu.</p>
3	Gwarancja	<p>1. Okres i zakres gwarancji</p> <p>1.1. Gwarancja musi obejmować zapewnienie dostępności najnowszych aktualizacji, poprawek</p>

bezpieczeństwa (w tym związanych z podatnościami typu CVE) i usprawnień funkcjonalnych wydawanych przez producenta/dostawcę w celu utrzymania pełnej funkcjonalności oprogramowania oraz jego bezpieczeństwa.

1.2. Okres gwarancji musi wynosić 36 (trzydzieści sześć) miesięcy, liczonych od daty podpisania protokołu odbioru końcowego systemu.

1.3. Aktualizacje i poprawki muszą być dostarczane bez dodatkowych kosztów dla Zamawiającego, a zasady ich wdrażania muszą być zawarte w dokumentacji technicznej.

2. Zasady zgłaszania awarii, usterek, błędów

2.1. Awarię, usterkę lub błąd w działaniu należy zgłaszać:

wysyłając wiadomość e-mail na dedykowany adres serwisowy Wykonawcy wskazany w umowie, lub poprzez dedykowaną aplikację webową/system zgłoszeniowy Wykonawcy.

2.2. Wykonawca jest zobowiązany do poinformowania Zamawiającego o każdej zmianie adresu e-mail czy dostępu do aplikacji serwisowej co najmniej 7 (siedem) dni przed planowaną zmianą. W przypadku niedopełnienia tej powinności za skuteczne uważa się wysłanie zgłoszenia na dotychczasowy adres lub do dotychczasowej aplikacji.

3. Potwierdzanie przyjęcia zgłoszenia

3.1. Wykonawca zobowiązuje się potwierdzić przyjęcie każdego zgłoszenia (niezależnie od formy – e-mail czy aplikacja webowa) w terminie nie dłuższym niż 4 (cztery) godziny od chwili jego otrzymania.

3.2. Za moment otrzymania zgłoszenia uważa się: chwilę wpływu wiadomości e-mail na serwer

pocztowy Wykonawcy (w przypadku zgłoszeń mailowych), chwilę prawidłowego zarejestrowania zgłoszenia w systemie (w przypadku aplikacji webowej).

3.3. Potwierdzenie przyjęcia zgłoszenia musi zawierać co najmniej:
datę i godzinę przyjęcia zgłoszenia,
unikalny identyfikator zgłoszenia (umożliwiający jego śledzenie),

4. Czas realizacji naprawy lub usunięcia usterki

4.1. Klasyfikacja

Awaria: całkowita niedostępność możliwości korzystania z oprogramowania, poważne naruszenie bezpieczeństwa (np. istotna podatność bezpieczeństwa), awaria uniemożliwiająca kontynuację kluczowych procesów Zamawiającego albo stwarzająca wysokie ryzyko utraty lub naruszenia integralności danych.

Usterka: nieprawidłowe działanie istotnej funkcjonalności systemu, które może znacząco utrudnić wykonywanie głównych zadań Zamawiającego, jednak nie prowadzi do całkowitego zatrzymania systemu ani utraty danych.

Błąd: usterka niezakłócająca w istotny sposób działania systemu ani niepowodująca utraty danych.

4.2. Czasy realizacji napraw lub usunięcia awarii, usterek, błędów

Awaria - wykonawca zobowiązany jest do podjęcia działań naprawczych niezwłocznie po otrzymaniu zgłoszenia, a usunięcie awarii (przywrócenie pełnej funkcjonalności i bezpieczeństwa systemu) musi nastąpić w ciągu maksymalnie 24 (siedemdziesięciu dwóch) godzin od momentu potwierdzenia przyjęcia zgłoszenia.

Usterka - wykonawca zobowiązany jest do usunięcia usterki w możliwie najkrótszym terminie, jednak nie dłuższym niż 5 dni roboczych od momentu potwierdzenia przyjęcia zgłoszenia.

Błąd - wykonawca zobowiązany jest do usunięcia błędu w terminie uzgodnionym z Zamawiającym,

		<p>jednak nie dłuższym niż 30 dni roboczych od momentu potwierdzenia przyjęcia zgłoszenia.</p> <p>5. Warunki dodatkowe (aktualizacje, komunikacja, informacje)</p> <p>5.1. Wszelkie aktualizacje i poprawki oprogramowania związane z bezpieczeństwem muszą być w okresie gwarancji udostępniane Zamawiającemu bez dodatkowych opłat.</p> <p>5.2. Cała komunikacja między Wykonawcą a Zamawiającym w ramach realizacji gwarancji (w tym zgłaszanie awarii, usterek, błędów, potwierdzanie przyjęcia zgłoszeń, informowanie o statusie naprawy lub usuwania błędów) musi odbywać się w języku polskim.</p> <p>5.3. Wykonawca jest zobowiązany do bieżącego informowania Zamawiającego o postępach w naprawie lub usuwaniu usterek, na każde żądanie Zamawiającego kierowane w formie elektronicznej lub pisemnej.</p>
4	Dokumentacja techniczna	<p>Zamawiający zastrzega, że w ramach dostarczanych licencji na oprogramowanie backupu, musi uzyskać pełne i nieograniczone prawa do korzystania z wszelkiej dokumentacji związanej z oprogramowaniem. Dokumentacja ta obejmuje, ale nie jest ograniczona do: instrukcji użytkownika i administratora, projektów technicznych, dokumentacji operacyjnej oraz wszelkich innych materiałów edukacyjnych i pomocniczych, które są niezbędne do efektywnego wykorzystania, utrzymania i zarządzania oprogramowaniem do backupu.</p> <p>Zamawiający otrzyma prawa do:</p> <ol style="list-style-type: none"> 1. Wykorzystywania dokumentacji w celach operacyjnych, szkoleniowych i wdrożeniowych w obrębie organizacji Zamawiającego. 2. Tworzenia kopii dokumentacji niezbędnych dla wewnętrznych potrzeb organizacyjnych. 3. Modyfikowania dokumentacji w zakresie

		<p>wymaganiem do dostosowania procedur i instrukcji do specyficznych potrzeb operacyjnych Zamawiającego.</p> <p>Wszelkie prawa autorskie do dokumentacji pozostają własnością producenta lub dostawcy rozwiązania, jednak Zamawiający otrzymuje licencję nieograniczoną czasowo i terytorialnie, zezwalającą na korzystanie z dokumentacji zgodnie z powyższymi warunkami. Dostawca zobowiązuje się dostarczyć dokumentację w formie elektronicznej w języku polskim lub angielskim. Dostawca musi zapewnić dostęp do aktualizacji dokumentacji przez okres obowiązywania wsparcia.</p>
5	Szacowana wielkość danych podlegających backupowi	48 TB
6	Wymóg kompatybilności i instalacji oprogramowania na dostarczonej platformie sprzętowej.	<p>Oprogramowanie musi być zainstalowane i w pełni funkcjonalne na platformie sprzętowej opisanej w Zadaniu 7 lub na serwerze opisanym w Zadaniu 1. Zamawiający nie narzuca architektury rozwiązania. Instalacja oraz konfiguracja oprogramowania muszą być przeprowadzone w sposób zapewniający maksymalną wydajność i stabilność zgodnie z rekomendacjami producenta oprogramowania i platformy sprzętowej.</p> <p>Dostawca oprogramowania zobowiązany jest do przeprowadzenia weryfikacji poprawności działania oprogramowania na wspomnianej platformie sprzętowej, włącznie z testami kompatybilności i wydajności. Dodatkowa weryfikacja nastąpi w ramach realizacji procedury odbioru systemu backupu opisanej w punkcie 34 niniejszej tabeli.</p> <p>Oprogramowanie musi wspierać scenariusz replikacji lub przesyłania kopii zapasowych do</p>

		fizycznie oddzielnej lokalizacji, połączonej światłowodem.
7	Kompatybilność z systemami przechowywania danych.	<p>Oprogramowanie musi być zdolne do tworzenia kopii zapasowych danych z urządzeń plikowych NAS, które używają protokołów SMB (Server Message Block). Model serwera plików wykorzystywanych przez zamawiającego: Synology RS1221RP+</p> <p>Oprogramowanie musi umożliwiać tworzenie kopii zapasowych bezpośrednio z serwerów plikowych działających na systemach operacyjnych Windows i Linux.</p> <p>Zamawiający dopuszcza stosowanie klientów.</p>
8	Odzyskiwanie danych	<ol style="list-style-type: none"> 1. Każde archiwum musi zawierać wszystkie niezbędne dane oraz metadane w taki sposób, aby można było je odzyskać. Archiwa muszą zawierać wszystkie informacje potrzebne do ich pełnego i niezależnego odzyskania. Obejmuje to nie tylko same zabezpieczone dane, ale również metadane, które opisują dane i ich strukturę. 2. Oprogramowanie musi posiadać mechanizmy kompresji danych, mające na celu zmniejszenie całkowitej wielkości archiwów backupowych. Włączenie kompresji nie może prowadzić do jakiegokolwiek utraty istniejących funkcjonalności oprogramowania, wymienionych w opisie przedmiotu zamówienia.
9	Backup maszyn wirtualnych oraz kompatybilność z platformą wirtualizacji	<p>Oprogramowanie musi być w pełni kompatybilne z serwerem i jego oprogramowaniem do wirtualizacji dostarczonym w ramach niniejszego zamówienia opisanym w Zadaniu 7. Środowisko backupowe oraz środowisko wirtualizacji muszą być w pełni ze sobą zintegrowane i przetestowane w ramach procedury odbioru systemu.</p> <p>Oprogramowanie musi umożliwiać wykonywanie pełnych kopii zapasowych całych maszyn wirtualnych bezpośrednio z poziomu warstwy</p>

		<p>wirtualizacyjnej. Backup musi obejmować całą zawartość dysków, konfigurację sprzętową, metadane oraz ustawienia sieciowe maszyn wirtualnych.</p> <p>System backupu musi umożliwiać pełne przywrócenie maszyn wirtualnych na tym samym lub innym hoście, z zachowaniem ich pełnej funkcjonalności.</p>
10	Integracja z chmurą	Oprogramowanie musi umożliwiać tworzenie repozytorium kopii bezpośrednio na zasobach chmurowych, takich jak np. Microsoft Azure Blob, Google Cloud Storage, Amazon S3.
11	Odtwarzanie danych	<p>Oprogramowanie do backupu musi oferować portal, umożliwiający użytkownikom samodzielne odtwarzanie wirtualnych maszyn, plików oraz baz danych Microsoft SQL, PostgreSQL, Firebird.</p> <p>W przypadku, gdy któraś z wymienionych baz danych nie jest wspierana przez dostarczone rozwiązanie, zamawiający dopuszcza alternatywne rozwiązanie umożliwiające backup niewspieranej bazy, pod warunkiem, że wykonawca dokona odpowiedniej konfiguracji lub zapewni niezbędne rozwiązanie, zapewniając pełną funkcjonalność i zgodność z wymaganiami dotyczącymi odtwarzania danych.</p>
12	Delegacja uprawnień	<p>Oprogramowanie musi oferować możliwość konfiguracji uprawnień dla różnych użytkowników lub grup użytkowników, umożliwiając im samodzielne odtwarzanie danych, co ma pozwalać na elastyczne zarządzanie dostępem do danych.</p> <p>Delegacja uprawnień musi być również wspierana przez funkcje monitorowania, które rejestrują wszelkie działania użytkowników w systemie w zakresie pozwalającym na śledzenie kto, kiedy i jakie operacje odtwarzania przeprowadził.</p>
13	Integracja z systemami zewnętrznymi.	Oprogramowanie musi być dostarczone wraz z pełną i szczegółową dokumentacją techniczną, która opisuje wszystkie dostępne interfejsy API lub opcje integracji z systemami zewnętrznymi, np. poprzez protokół Syslog. Dokumentacja musi zawierać przykłady użycia, przewodniki integracyjne, opisy metod, parametrów, możliwych odpowiedzi i błędów, a także najlepsze praktyki

		<p>związane z integracją i automatyzacją z użyciem API lub np. Syslog. Wykonawca musi dokonać integracji oprogramowania z oprogramowaniem opisanym w Zadaniu 8 w minimalnym zakresie:</p> <ul style="list-style-type: none"> • Identyfikator zadania backupu: Unikalny numer lub kod przypisany do każdego zadania backupowego, umożliwiający jednoznaczną identyfikację. • Status zadania: Informacja o wyniku operacji, np. rozpoczęcie, zakończenie sukcesem, zakończenie z błędem, przerwanie. • Czas rozpoczęcia i zakończenia: Dokładne znaczniki czasu określające, kiedy zadanie zostało rozpoczęte i zakończone. • Nazwa i lokalizacja źródła danych: Identyfikacja serwera, urządzenia lub aplikacji, z której dane są kopiowane, wraz z informacją o lokalizacji danych. • Nazwa i lokalizacja docelowa backupu: Informacja o miejscu, gdzie kopia zapasowa została zapisana, np. nazwa serwera backupowego, ścieżka do pliku. • Wielkość przetworzonych danych: Ilość danych (w MB, GB) skopiowanych podczas zadania backupu. • Czas trwania zadania: Łączny czas, jaki upłynął od rozpoczęcia do zakończenia zadania. • Użytkownik inicjujący: Nazwa użytkownika lub identyfikator procesu, który zainicjował zadanie backupu. • Lista plików lub baz danych objętych backupem: Szczegółowy wykaz elementów uwzględnionych w kopii zapasowej. <p>Zamawiający dopuszcza dokumentację w języku polskim lub angielskim.</p>
14	Wbudowane mechanizmy backupu konfiguracji	<p>Oprogramowanie musi posiadać funkcje umożliwiające zapisywanie ustawień i konfiguracji oprogramowania do backupu. Musi to obejmować wszystkie kluczowe parametry, ustawienia</p>

		użytkownika oraz wszelkie inne dane konfiguracyjne, które są niezbędne do prawidłowego funkcjonowania oprogramowania.
15	Szyfrowanie plików backupu	Oprogramowanie musi mieć funkcjonalność do szyfrowania plików backupu.
16	Dostęp do konsoli administracyjnej	Oprogramowanie musi posiadać architekturę umożliwiającą instalację konsoli administracyjnej. Zamawiający dopuszcza konsolę administracyjną opartą na przeglądarce internetowej.
17	Mechanizm śledzenia zmienionych plików	Oprogramowanie musi zawierać mechanizmy śledzenia zmienionych plików. Oprogramowanie musi automatycznie identyfikować i archiwizować tylko te pliki, które zostały zmodyfikowane od czasu ostatniego backupu. Mechanizmy te muszą umożliwić szybkie przywracanie danych w przypadku awarii, co ma gwarantować, że tylko najnowsze zmiany w danych będą chronione i szybko odzyskiwane.
18	Tworzenie kopii zapasowych z wykorzystaniem snapshotów	Oprogramowanie musi umożliwiać tworzenie kopii zapasowych danych przez bezpośrednie wykorzystanie snapshotów.
19	Schemat retencji	Oprogramowanie musi oferować możliwość konfiguracji i zarządzania polityką retencji danych zgodnie ze schematem GFS (Grandfather-Father-Son). Oprogramowanie musi umożliwiać elastyczne ustawienia retencji dla różnych poziomów backupu: dziennego (Son), tygodniowego (Father) i miesięcznego (Grandfather).
20	Przywracanie plików i folderów	Oprogramowanie musi umożliwiać odtwarzanie plików oraz folderów wraz z ich uprawnieniami bezpośrednio na serwer produkcyjny. Funkcjonalność musi być dostępna bez względu na wielkość i liczbę przywracanych plików.
21	Monitorowanie wydajności i zarządzania zadaniami w systemie	Oprogramowanie musi być wyposażone w narzędzia monitorowania statystyki dotyczące ilości zabezpieczanych danych oraz wydajności operacji takich jak tworzenie kopii zapasowych. Wymagane funkcje monitorowania muszą obejmować:

		<ol style="list-style-type: none"> 1. statystyki dotyczące całkowitej ilości zabezpieczanych danych, z możliwością wglądu w historię i tendencje zmian. 2. szczegółowy przegląd statusu zadań związanych z kopiami zapasowymi.
22	Harmonogramowanie i zarządzanie backupami	<p>Wymagane funkcjonalności muszą obejmować:</p> <ol style="list-style-type: none"> 1. konfigurowanie i zarządzanie harmonogramami, pozwalające na automatyczne przeprowadzanie operacji backupu zgodnie z zdefiniowanymi interwałami czasowymi. 2. możliwość szybkiego tworzenia i uruchamiania zadań backupu ad-hoc, umożliwiających reagowanie na specyficzne potrzeby i sytuacje.
23	Odtwarzanie systemu po awarii	<p>Oprogramowanie musi posiadać funkcjonalność umożliwiającą odtwarzanie po awarii konfiguracji serwera zarządzającego procesem tworzenia kopii bezpieczeństwa i archiwizacji danych. Oprogramowanie musi zapewnić efektywne i szybkie przywrócenie ustawień oraz konfiguracji serwera zarządzającego w przypadku jego awarii, gwarantując minimalny czas przestoju oraz zapewniając ciągłość działania procesów backupowych. System musi obsługiwać pełne odtworzenie funkcji serwera, w tym wszystkich jego zasad, harmonogramów i parametrów operacyjnych, co umożliwi nieprzerwane prowadzenie operacji backupu i archiwizacji danych zgodnie z ustalonymi procedurami.</p>
24	Deduplikacja	<p>Oprogramowanie musi oferować funkcjonalność deduplikacji danych, która pozwala na przechowywanie jedynie unikalnych bloków danych. Proces deduplikacji musi być realizowany na poziomie blokowym.</p>
25	Typy backupów	<p>Oprogramowanie musi zapewniać możliwość wykonywania różnych typów kopii zapasowych, w tym backupu pełnego, przyrostowego, różnicowego.</p>

		Oprogramowanie musi umożliwiać elastyczne zarządzanie tymi typami backupów w celu optymalizacji procesów ochrony danych i redukcji obciążeń sieciowych oraz czasu potrzebnego na backup.
26	Kopie baz danych	<p>Oprogramowanie musi umożliwiać wykonywanie kopii zapasowych danych z baz danych MySQL, PostgreSQL, MS SQL oraz Firebird, działających na dowolnej platformie systemu operacyjnego (Windows, Linux). Realizacja backupu musi odbywać się za pomocą dedykowanego agenta bazodanowego. Transfer danych musi być przeprowadzony bezpośrednio z agenta bazodanowego do systemu backupowego, bez pośredniczenia dysków lokalnych.</p> <p>W przypadku, gdy dostarczone oprogramowanie nie posiada dedykowanego agenta dla którejkolwiek z wymienionych baz danych, Zamawiający dopuszcza możliwość wykorzystania alternatywnego rozwiązania, pod warunkiem, że wykonawca dokona niezbędnej konfiguracji tego rozwiązania oraz przekaże pełną dokumentację opisującą sposób realizacji i zarządzania backupem. Alternatywne rozwiązanie musi zapewniać równoważny poziom funkcjonalności, bezpieczeństwa i efektywności backupu, zgodnie z wymaganiami Zamawiającego.</p> <p>W przypadku proponowania alternatywnych rozwiązań, dostawca jest zobowiązany do przedstawienia szczegółowej dokumentacji technicznej i wyników testów potwierdzających równoważność tych rozwiązań z wymaganiami określonymi w specyfikacji. Dodatkowa weryfikacja nastąpi w ramach realizacji procedury odbioru systemu backupu opisanej w punkcie 34 niniejszej tabeli.</p>
27	Odtwarzanie kopii baz danych	Oprogramowanie musi umożliwiać odtwarzanie danych z kopii zapasowych baz danych takich jak

		<p>MS SQL, MySQL, PostgreSQL oraz Firebird bezpośrednio poprzez konsolę administracyjną. Funkcjonalność ta musi umożliwiać przywracanie danych bez konieczności manualnego konfigurowania dodatkowych skryptów.</p> <p>W przypadku, gdy dostarczone oprogramowanie nie wspiera bezpośredniej obsługi którejkolwiek z wymienionych baz danych, Zamawiający dopuszcza stosowanie skryptów lub agentów. Jeżeli przywracanie będzie wymagało opracowania skryptów, to musi je stworzyć wykonawca, musi je również wdrożyć, przetestować, a także dostarczyć kompletną dokumentację opisującą ich działanie i sposób użycia. Skrypty te muszą zapewnić efektywne i bezpieczne przywracanie danych.</p>
28	Testowanie backupów	<p>Oprogramowanie musi umożliwiać regularne testowanie, aby zapewnić, że tworzone backupy są kompletnie i prawidłowo wykonywane oraz mogą być skutecznie przywracane w przypadku utraty danych. Testowanie musi być możliwe w ramach dostarczonej przez wykonawcę infrastruktury.</p>
29	Elastyczność i skalowalność	<p>Oprogramowanie do backupu musi być zaprojektowane z myślą o przyszłych wymaganiach i możliwościach skalowania, aby można było dostosować je do rosnących lub zmieniających się potrzeb organizacji.</p> <p>Oprogramowanie musi umożliwiać skalowanie pojemności dyskowej. Dostawca musi przedstawić dokumentację techniczną opisującą proces rozszerzania zasobów.</p>
30	Możliwość kontrolowania działań	<p>Oprogramowanie musi zapewniać szczegółowe logowanie wszystkich operacji związanych z danymi, w tym informacje o tym, kto, kiedy i co zrobił z backupami. Logi te muszą być dostępne i czytelne dla upoważnionych, umożliwiając monitorowanie zgodności z politykami i procedurami bezpieczeństwa.</p>
31	Rejestrowanie, weryfikacja i	<p>Oprogramowanie musi automatycznie rejestrować</p>

	walidacja zmian	wszystkie działania związane z krytycznymi funkcjami, w tym kto, kiedy i jakie działania wykonał.
32	Synchronizacja zegara systemowego	Oprogramowanie musi synchronizować wszystkie wewnętrzne zegary systemowe z centralnym, wiarygodnym źródłem czasu, takim jak serwery czasu NTP (Network Time Protocol) lub inny odpowiedni protokół.
33	Zapewnienie kompatybilności i gotowości użytkowej	Dostarczone oprogramowanie musi być w pełni kompatybilne z sprzętem i oprogramowaniem opisanym w zadaniu 1, zadaniu 8, zadaniu 7, system Gmina 3 firmy ZETO Koszalin (obsługujący finanse, podatki, opłaty, płace, windykację i księgowość budżetową), systemem eKancelaria, bazy danych wykorzystywane przez zamawiającego: Microsoft SQL, PostgreSQL, Firebird, serwer Synology RS1221RP+. Wykonawca jest odpowiedzialny za kompleksową konfigurację oprogramowania wraz z dostarczonym sprzętem, aby całość była w pełni gotowa do użytku przez zamawiającego od momentu instalacji. Konfiguracja ta musi zapewnić, że wszystkie komponenty sprzętowe i oprogramowanie działają sprawnie i efektywnie współpracują, co pozwoli zamawiającemu na natychmiastowe rozpoczęcie pracy z systemem bez potrzeby dodatkowych ustawień czy modyfikacji.
34	Wdrożenie	<p>1. Instalacja i konfiguracja oprogramowania</p> <p>a. Wykonawca dokona instalacji i konfiguracji oprogramowania do backupu na platformie sprzętowej opisanej w Zadaniu 7 lub serwerze opisanym w Zadaniu 1, zgodnie z rekomendacjami producenta oprogramowania oraz zgodnie z wymaganiami określonymi w niniejszym załączniku. Zamawiający nie narzuca architektury rozwiązania.</p> <p>b. Proces instalacji i konfiguracji musi</p>

uwzględniać co najmniej :

- Integrację z istniejącymi serwerami i usługami wymagającymi backupu (w tym baz danych, maszyn wirtualnych, urządzeń NAS i serwerów plików).
- Ustawienie mechanizmów retencji, schematów backupów (pełny, różnicowy, przyrostowy) oraz harmonogramu zadań backupowych.
- Włączenie deduplikacji i kompresji danych.
- Zapewnienie szyfrowania plików backupu.
- Konfigurację kont i uprawnień dla administratora oraz ewentualnych użytkowników uprawnionych do samodzielnego odtwarzania danych.

2. Integracja z systemami zewnętrznymi

- a. Wykonawca dokona integracji oprogramowania z rozwiązaniami wskazanymi w Zadaniu 8 i innych zadaniach, jeżeli wymagają tego warunki zamówienia.
- b. Wykonawca jest zobowiązany do dostarczenia Zamawiającemu pełnej dokumentacji integracji (np. opis dostępnych interfejsów API, konfiguracji Syslog).

3. Instruktaż i przekazanie wiedzy

W ramach wdrożenia Wykonawca przeprowadzi instruktaż dla informatyka zamawiającego co najmniej z zakresu:

- obsługi i zarządzania oprogramowaniem backupowym,
- konfiguracji i definiowania zadań backupu,
- przywracania danych, w tym baz danych, maszyn wirtualnych oraz plików,
- procedur testowania backupów i odtwarzania systemów,
- interpretacji logów, raportów i alertów

		<p>związanych z systemem backupu,</p> <ul style="list-style-type: none"> ▪ Szkolenie musi obejmować również prezentację najlepszych praktyk i rekomendacji producenta w zakresie eksploatacji i utrzymania systemu backupu. ▪ Minimalna ilość godzin szkolenia: 8 godzin. ▪ Ilość osób z którymi zostanie przeprowadzony instruktaż: 1.
35	Procedura odbioru oprogramowania backupu	<ol style="list-style-type: none"> 1. Zamawiający, przy współpracy z Wykonawcą, opracuje scenariusze testów akceptacyjnych, które będą uwzględniać wszystkie wymagane funkcjonalności systemu, zapisane w specyfikacji zamówienia. 2. Testy akceptacyjne będą przeprowadzone przez zespół Zamawiającego ze wsparciem technicznym ze strony Wykonawcy, co ma na celu weryfikację zgodności systemu z ustalonymi wymaganiami. 3. Wyniki testów będą dokumentowane przez Zamawiającego, w celu zapewnienia rzetelności procesu akceptacji. 4. Po zakończeniu testów i potwierdzeniu, że system spełnia ustalone kryteria akceptacji, Zamawiający sporządzi protokół odbioru końcowego. 5. Protokół odbioru musi być akceptowany i podpisany przez obie strony, co formalnie potwierdzi przyjęcie systemu backupu do eksploatacji.

3.3 Zadanie 3: UPS stanowiskowe – 10 szt.

Komentarz [AG1]:

L.p.	Wymaganie	Opis wymagania
1	Cel	Celem zadania jest zapewnienie ciągłości pracy komputerów i urządzeń biurowych w Urzędzie Miejskim w Białym Borze w przypadku

		<p>krótkotrwałych przerw w dostawie energii elektrycznej.</p> <p>Zakup indywidualnych UPS-ów ma umożliwić pracownikom bezpieczne zapisanie danych, zamknięcie systemów i ograniczyć ryzyko uszkodzenia sprzętu lub utraty danych.</p>
2	Moc wyjściowa AC	Urządzenie musi posiadać moc znamionową nie mniejszą niż 1000 W.
3	Topologia	Urządzenie musi działać w trybie Line-Interactive.
4	Wyjścia AC	Urządzenie musi posiadać co najmniej cztery gniazda wyjściowe AC (IEC C13 lub Schuko).
5	Zakres napięcia wyjściowego	Urządzenie musi zapewniać napięcie wyjściowe w zakresie 220V-240V.
6	Czas podtrzymania	Urządzenie musi zapewniać czas podtrzymania dla obciążenia 50% wynoszący co najmniej 5 min.
7	Zabezpieczenia	Urządzenie musi być wyposażone w zabezpieczenia przeciwprzepięciowe oraz przeciążeniowe.
8	Interfejs komunikacyjny	Urządzenie musi posiadać interfejs USB do komunikacji z systemem zarządzania energią.
9	Sygnalizacja pracy	Urządzenie musi posiadać wyświetlacz LCD lub diody LED do monitorowania pracy.
10	Gwarancja	Minimalny okres gwarancji na urządzenie musi wynosić 24 miesiące. Okres gwarancji rozpoczyna się w dniu podpisania przez obie strony protokołu odbioru, potwierdzającego poprawną dostawę i uruchomienie urządzeń.
11	Instalacja i uruchomienie	Wykonawca musi dostarczyć i zainstalować UPS-y we wskazanych pomieszczeniach w siedzibie zamawiającego.
12	Odbiory	Zamawiający uzna wymaganie za spełnione, jeżeli Wykonawca załączy do oferty karty katalogowe, broszury techniczne lub inne dokumenty producenta potwierdzające zgodność oferowanego urządzenia z wymaganiami.
13	Ilość szt.	10

3.4 Zadanie 4: Zakup dodatkowego urządzenia klasy UTM plus licencje dla 2 urządzeń

L.p.	Wymaganie	Opis wymagania
1	Przedmiot zamówienia	<ol style="list-style-type: none"> 1. Dostawa urządzenia FortiGate FG-60F lub równoważnego wraz z 2 licencjami. Druga licencja będzie wykorzystana do obecnie posiadanego urządzenia. Opis równoważności opisano w pkt od 7 do 20 niniejszej tabeli. 2. Urządzenie musi być fabrycznie nowe i kompletne (z pełnym okablowaniem, w tym przewód zasilający) oraz oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta oraz muszą pochodzić z legalnego źródła zapewniającego zgodność z prawem UE, z uwzględnieniem wymogów gwarancyjnych producenta. 3. Urządzenie i oprogramowanie muszą być wolne od wad oraz od obciążeń prawami osób trzecich oraz pochodzić z legalnych źródeł. 4. W przypadku wyboru urządzenia równoważnego, oprócz 1 licencji FortiGate FG-60F dla starego urządzenia, należy zapewnić dedykowane licencje i usługi wsparcia producenta na nowy sprzęt, tak aby w pełni spełnić wymagania niniejszego zamówienia. 5. Jeżeli oferowana licencja (lub jej komponent) obejmuje subskrypcję na aktualizacje bądź wsparcie producenta, wówczas subskrypcja ta musi być ważna przez okres 8. miesięcy od dnia podpisania protokołu odbioru, jednakże nie dłużej niż do dnia 30kwietnia 2026.
2	Cel zamówienia	Zamówienie ma na celu wdrożenie rozwiązania służącego do kontroli ruchu sieciowego oraz skutecznego blokowania potencjalnych zagrożeń zewnętrznych i wewnętrznych poprzez zakup i wdrożenie nowych urządzeń UTM (Unified Threat Management).
3	Klaster	Urządzenia UTM muszą być skonfigurowane do pracy w klastrze, z obecnie posiadanym urządzeniem FortiGate FG-60F co ma zapewniać wyższą dostępność i nieprzerwaną ochronę w przypadku awarii lub aktualizacji jednego z urządzeń. Praca w klastrze wynika ze względów bezpieczeństwa i szybkości przełączania w razie awarii.
4	Warunki realizacji zamówienia	<ol style="list-style-type: none"> 1. Dostawca jest odpowiedzialny za dostarczenie urządzenia. Dostawa musi zawierać wszystkie niezbędne komponenty i akcesoria wymagane do pełnej funkcjonalności urządzeń. 2. Dostawca ma obowiązek zabezpieczyć i przenieść wszystkie obecnie działające polityki bezpieczeństwa z istniejących urządzeń UTM na nowo dostarczone urządzenie (posiadane urządzenie to: FortiGate FG-60F). Proces ten musi być

		wykonany w taki sposób, aby zapewnić ciągłość ochrony i minimalizować ryzyko wystąpienia luk w zabezpieczeniach podczas konfiguracji nowego urządzenia.
5	Gwarancja	<ol style="list-style-type: none"> 1. Dostarczone rozwiązanie musi być objęte gwarancją przez okres 12 miesięcy od daty dokonania odbioru przedmiotu umowy. 2. W ramach gwarancji dostawca jest zobowiązany do zapewnienia dostępu do wszystkich aktualizacji oprogramowania dostarczonych przez producenta urządzeń, które mają na celu zwiększenie bezpieczeństwa oraz naprawę znanych błędów i podatności. 3. Dostawca lub producent musi zagwarantować udostępnienie, dostarczenie oraz instalację sprzętu zastępczego na czas naprawy w ciągu 24 godzin od momentu potwierdzenia zasadności zgłoszenia. 4. Czas reakcji serwisu nie może być dłuższy niż 4 godziny.
6	Wsparcie	<ol style="list-style-type: none"> 1. Wsparcie musi być realizowane przez okres 8 miesięcy, nie dłużej niż do 30 kwietnia.2026 r. od dnia podpisania protokołu odbioru przedmiotu umowy. 2. Wsparcie musi obejmować dostęp do wsparcia technicznego dostępnego od poniedziałku do piątku w dni robocze w godzinach od 7.00 do 15.00. Wsparcie to musi obejmować pomoc telefoniczną, przez e-mail oraz zdalne sesje diagnostyczne, umożliwiające szybkie rozwiązywanie problemów i wątpliwości związanych z funkcjonowaniem dostarczonego urządzenia. Wsparcie techniczne musi być realizowane w języku polskim. 3. Wsparcie musi obejmować m.in. konsultacje techniczne (telefoniczne/mailowe) dla administratorów Zamawiającego, pomoc przy ewentualnej początkowej konfiguracji lub rozwiązywaniu problemów z działaniem urządzenia, niezależnie od uprawnień gwarancyjnych.
7	Opis równoważności - wymagania ogólne	<p>Urządzenie UTM musi spełniać poniższe kryteria funkcjonalne i techniczne:</p> <ol style="list-style-type: none"> 1. UTM musi obsługiwać pracę w jednym z trzech trybów: <ul style="list-style-type: none"> • Router z funkcją NAT, • Tryb transparentny, 2. UTM musi umożliwiać tworzenie co najmniej dwóch oddzielnych (fizycznych lub logicznych) instancji dla takich funkcji jak: <ul style="list-style-type: none"> • Routing, • Firewall,

		<ul style="list-style-type: none"> • IPSec VPN, • Antywirus, • IPS (Intrusion Prevention System), • Kontrola aplikacji. <p>3. Urządzenia muszą pozwalać na przypisanie dwóch administratorów do zarządzania poszczególnymi instancjami.</p> <p>4. Urządzenie musi wspierać protokoły IPv4 oraz IPv6, zapewniając funkcjonalności w zakresie:</p> <ul style="list-style-type: none"> • Firewalla, • Ochrony w warstwie aplikacji, • Routingu dynamicznego. <p>Rozwiązania równoważne muszą spełniać powyższe wymagania techniczne i funkcjonalne, aby zapewnić ciągłość, efektywność oraz optymalizację działania systemów bezpieczeństwa w infrastrukturze zamawiającego. Równoważne produkty lub rozwiązania zostaną zaakceptowane pod warunkiem, że zapewnią te same parametry funkcjonalne i techniczne, co wymienione w przedmiocie zamówienia oraz w pełni zintegrują się z istniejącą infrastrukturą sieciową zamawiającego.</p>
8	Opis równoważności w zakresie redundancji, monitoringu i wykrywania awarii	<p>1. Urządzenie musi oferować funkcje filtrowania i ochrony przed nieautoryzowanym dostępem, zarówno w ruchu przychodzącym, jak i wychodzącym.</p> <p>2. Wymagana jest możliwość tworzenia bezpiecznych połączeń VPN z wykorzystaniem protokołu IPSec, umożliwiającą szyfrowane połączenie między różnymi lokalizacjami.</p> <p>3. Urządzenie musi pozwalać na kontrolę i zarządzanie aplikacjami działającymi w sieci Urzędu Miejskiego w Białym Borze, w celu zapobiegania wykorzystaniu aplikacji do przeprowadzania ataków lub wycieku danych.</p> <p>4. Urządzenie musi posiadać mechanizm zapobiegania intruzom (IPS), który aktywnie monitoruje sieć w poszukiwaniu potencjalnych zagrożeń i automatycznie reaguje na wykryte ataki.</p> <p>5. Urządzenie musi posiadać możliwość konfiguracji w trybach Active-Active lub Active-Passive dla zapewnienia ciągłości działania i optymalizacji wydajności, z funkcją synchronizacji sesji w obu trybach.</p> <p>6. Wymagana jest zdolność urządzenia do monitorowania stanu i wydajności realizowanych połączeń VPN, w celu zapewnienia ich stabilności i bezpieczeństwa.</p>
9	Opis równoważności w zakresie interfejsów, zasilania	<p>Urządzenie musi spełniać poniższe wymagania równoważności:</p> <p>1. Interfejsy:</p> <ul style="list-style-type: none"> • Minimum 2 porty WAN, minimum 1 port DMZ, minimum 5 ethernet, minimum 2 porty Link <p>2. Zasilanie</p> <p>Urządzenie musi być wyposażone w standardowe zasilanie AC dedykowane przez producenta urządzenia.</p>

10	Opis równoważności w zakresie parametrów wydajnościowych	<ol style="list-style-type: none"> 1. Wydajność z włączoną kontrolą aplikacji musi wynosić minimum 1.8 Gbps. 2. Wydajność szyfrowania IPSec VPN musi wynosić minimum 6.5 Gbps. 3. Wydajność modułu IPS (Intrusion Prevention System) musi wynosić minimum 1.4 Gbps. 4. Wydajność z włączonymi funkcjami IPS, kontrolą aplikacji i antywirusem musi wynosić minimum 630 Mbps. 5. Wydajność inspekcji komunikacji szyfrowanej SSL musi wynosić minimum 630 Mbps dla ruchu HTTP.
11	Opis równoważności w zakresie funkcji systemu bezpieczeństwa	<p>Urządzenie równoważne musi realizować wszystkie poniższe funkcje:</p> <ol style="list-style-type: none"> 1. posiadać zaporę ogniową, zapewniającą zaawansowaną analizę i filtrację ruchu sieciowego, 2. posiadać możliwość zarządzania i kontrolowania dostępu do aplikacji w sieci, 3. posiadać zabezpieczenie transmisji danych za pomocą szyfrowanych połączeń IPSec VPN, 4. posiadać funkcje ochrony Intrusion Prevention System (IPS), zapewniający ochronę przed zaawansowanymi atakami i zagrożeniami, 5. posiadać funkcjonalności związane z kontrolą stron WWW wykorzystując filtrację i kontrolę dostępu do stron internetowych, 6. posiadać narzędzia do inspekcji ruchu szyfrowanego protokołem SSL w tym narzędzia do przeglądania i kontroli ruchu szyfrowanego dla protokołów HTTP, 7. posiadać funkcjonalność automatyzacji działań, posiadać wbudowane mechanizmy umożliwiające automatyczne wykonywanie określonych akcji po wystąpieniu wybranego zdarzenia, takiego jak naruszenie polityki bezpieczeństwa.
12	Opis równoważności w zakresie polityk, firewall	<p>Urządzenie równoważne musi oferować:</p> <ol style="list-style-type: none"> 1. możliwość definiowania reguł na podstawie adresów IP, użytkowników, protokołów, usług sieciowych, aplikacji oraz zbiorów aplikacji. 2. rejestrować zdarzenia i odpowiednie reakcje zabezpieczeń na wykryte zagrożenia, 3. filtrować ruch w zależności od kraju pochodzenia lub przeznaczenia adresów IP, 4. posiadać możliwość tworzenia stref bezpieczeństwa takich jak DMZ, WAN, dostosowanych do potrzeb organizacji,
13	Opis równoważności w zakresie routingu	<p>Urządzenia równoważne muszą spełniać poniższe wymagania funkcjonalne:</p> <ol style="list-style-type: none"> 1. posiadać wsparcie dla konfiguracji statycznych tras routingu, 2. posiadać funkcjonalność pozwalającą na selektywne filtrowanie tras rozgłaszanych przez protokoły dynamicznego routingu, 3. posiadać możliwość korzystania z wielu równoważnych tras w tablicy routingu, co ma pozwalać na optymalizację

		wykorzystania łącz i zwiększenie odporności na awarie.
14	Opis równoważności w zakresie ochrony przed zagrożeniami typu malware	<p>Urządzenie równoważne musi spełniać poniższe wymagania funkcjonalne:</p> <ol style="list-style-type: none"> 1. musi posiadać możliwość skanowania ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach, np. FTP na porcie 2021, 2. obsługiwać skanowanie dla protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP 3. musi posiadać funkcjonalność automatycznej aktualizacji bazy sygnatur wirusów zgodnie z harmonogramem ustalonym przez administratora.
15	Opis równoważności w zakresie ochrony przed zagrożeniami	<p>Urządzenie równoważne musi spełniać poniższe wymagania funkcjonalne:</p> <ol style="list-style-type: none"> 1. urządzenie musi bazować na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych, aby skutecznie chronić przed różnorodnymi zagrożeniami (IPS), 2. urządzenie musi posiadać zabezpieczenia obejmujące aplikacje działające na niestandardowych portach, zapewniając ochronę niezależnie od używanej konfiguracji sieciowej, 3. urządzenie musi dysponować bazą sygnatur ataków, która jest aktualizowana automatycznie zgodnie z harmonogramem definiowanym przez administratora, 4. administrator systemu musi mieć możliwość definiowania własnych wyjątków, co ma pozwalać na dostosowanie ochrony do specyficznych potrzeb organizacji, 5. urządzenie musi oferować wykrywanie anomalii w protokołach i ruchu sieciowym, zapewniając podstawową ochronę przed atakami typu DoS i DDoS, 6. urządzenie musi umożliwiać wykrywanie i blokowanie komunikacji C&C do sieci botnet, zabezpieczając przed zaawansowanymi zagrożeniami, 7. urządzenie musi posiadać możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie, co ma umożliwiać elastyczne zarządzanie bezpieczeństwem.
16	Opis równoważności w zakresie kontroli aplikacji	<p>Rozwiązanie równoważne musi spełniać poniższe wymagania funkcjonalne:</p> <ol style="list-style-type: none"> 1. urządzenie musi posiadać funkcjonalność kontroli ruchu na podstawie głębokiej analizy pakietów, nie opierając się wyłącznie na wartościach portów TCP/UDP, co ma pozwalać na dokładniejsze monitorowanie i zarządzanie aplikacjami działającymi w sieci, 2. urządzenie musi posiadać bazę sygnatur aplikacji, która musi być regularnie aktualizowana automatycznie zgodnie z harmonogramem ustalonym przez administratora, co ma zapewnić aktualność i skuteczność mechanizmów kontroli, 3. baza sygnatur musi zawierać kategorie aplikacji istotne z

		<p>punktu widzenia bezpieczeństwa, takie jak proxy i P2P, umożliwiając skuteczną ochronę przed zagrożeniami,</p> <ol style="list-style-type: none"> 4. administratorzy systemu muszą mieć możliwość definiowania wyjątków, co ma umożliwiać dostosowanie systemu do specyficznych potrzeb organizacji, 5. urządzenie musi posiadać możliwość blokowania aplikacji działających na niestandardowych portach, zwiększając bezpieczeństwo sieci, 6. urządzenie musi posiadać możliwość określenia dopuszczalnych protokołów na danym porcie i blokowania pozostałych protokołów korzystających z tego portu, np. dopuszczenie tylko HTTP na porcie 80, co ma pozwalać na precyzyjne zarządzanie ruchem sieciowym.
17	Opis równoważności w zakresie kontroli www	<p>Urządzenia równoważne muszą spełniać poniższe wymagania funkcjonalne:</p> <ol style="list-style-type: none"> 1. urządzenia muszą korzystać z bazy adresów URL, pogrupowanych w kategorii tematyczne, co ma umożliwiać efektywne filtrowanie treści, 2. dostępne kategorie filtrowania muszą obejmować: malware, phishing, spam, Dynamic DNS, proxy, co ma zapewnić ochronę przed różnymi zagrożeniami internetowymi, 3. filtr musi obejmować kategorie stron zabronionych prawem, np. hazard, 4. administratorzy systemu muszą mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków, w tym białych i czarnych list dla adresów URL, co ma pozwalać na elastyczne dostosowanie polityk dostępu, 5. filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron, w tym definiowanie stron z użyciem wyrażeń regularnych (Regex), 6. urządzenia muszą posiadać możliwość wykonania akcji typu "Warning" (ostrzeżenie), gdzie użytkownik musi potwierdzić chęć otwarcia żądanej strony, 7. administratorzy muszą mieć możliwość definiowania komunikatów zwracanych użytkownikowi w zależności od akcji podejmowanych przez moduł filtrowania, 8. urządzenia muszą posiadać funkcjonalność pozwalającą na określenie, dla których kategorii URL lub wskazanych adresów URL nie będzie realizowana inspekcja szyfrowanej komunikacji, co ma zapewniać ochronę prywatności tam, gdzie jest to wymagane.
18	Opis równoważności w zakresie uwierzytelniania użytkowników w ramach sesji	<p>Urządzenie równoważne musi spełniać poniższe wymagania funkcjonalne:</p> <ol style="list-style-type: none"> 1. urządzenie musi mieć możliwość uwierzytelniania użytkowników przy użyciu haseł statycznych przechowywanych zarówno w lokalnej bazie systemu, jak i w bazach zgodnych z LDAP, 2. urządzenie musi posiadać możliwość implementacji uwierzytelniania dwuskładnikowego,

19	Opis równoważności w zakresie zarządzania	<p>Urządzenie równoważne musi spełniać poniższe wymagania funkcjonalne:</p> <ol style="list-style-type: none"> 1. urządzenie musi posiadać możliwość zarządzania lokalnego za pomocą protokołów HTTPS i SSH, 2. urządzenie musi korzystać z szyfrowania komunikacji między elementami systemu zabezpieczeń a platformami centralnego zarządzania, co zapewnia ochronę przed nieautoryzowanym dostępem, 3. urządzenie musi posiadać możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego, zwiększającego bezpieczeństwo zarządzania systemem, 4. urządzenie musi współpracować z rozwiązaniami służącymi do monitorowania za pomocą protokołów SNMP w wersjach 2c i 3, 5. urządzenie musi posiadać wbudowane narzędzia diagnostyczne takie jak ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall, 6. urządzenie musi udostępniać API do zarządzania systemem przez oprogramowanie firm trzecich, wraz z pełną dokumentacją dostarczoną przez producenta, 7. urządzenie musi posiadać rozwiązanie ograniczające zarządzanie systemem tylko do określonych adresów źródłowych IP, co ma zwiększać bezpieczeństwo przez ograniczenie dostępu do zaufanych lokalizacji.
20	Opis równoważności w zakresie logowania	<p>Rozwiązanie równoważne musi spełniać poniższe wymagania funkcjonalne:</p> <ol style="list-style-type: none"> 1. urządzenie musi zapewniać możliwość logowania do serwera SYSLOG, 2. urządzenie musi posiadać możliwość przesyłania SYSLOG do zewnętrznych systemów.
21	Dokumentacja	<p>Wszystkie funkcje i parametry dostarczonych urządzeń muszą być opisane w oficjalnej dokumentacji, która jest publicznie dostępna lub musi być przekazana zamawiającemu w postaci elektronicznej np. pdf, docx, odt. Dokumentacja ta musi zawierać szczegółowe informacje na temat specyfikacji technicznych, możliwości systemu oraz instrukcje użytkowania. Dokumentacja musi być dostępna w językach: polskim lub angielskim.</p>
22	Wdrożenie	<p>Dostawca jest zobowiązany do przeprowadzenia pełnej procedury wdrożenia urządzenia UTM w infrastrukturze zamawiającego.</p> <p>Procedura wdrożenia musi obejmować następujące etapy:</p> <ol style="list-style-type: none"> 1. Przeprowadzenie szczegółowej analizy istniejącej infrastruktury sieciowej zamawiającego oraz obowiązujących polityk w obecnym urządzeniu UTM. Na podstawie wyników analizy, dostawca wspólnie z zamawiającym opracuje plan wdrożenia, który zminimalizuje ryzyko wystąpienia przerw w działaniu systemów.

		<p>2. Przeniesienie wszystkich istniejących polityk bezpieczeństwa z dotychczas używanego urządzenia UTM na nowe urządzenie. Proces ten musi być przeprowadzony w sposób zapewniający pełną zgodność polityk oraz o ile to możliwe ich nieprzerwane działanie.</p> <p>3. Konfiguracja nowych urządzeń UTM zgodnie z przeniesionymi politykami oraz integracja z istniejącą infrastrukturą sieciową.</p> <p>4. Wszystkie działania wdrożeniowe muszą być ściśle monitorowane i dokumentowane.</p>
23	Integracje	<p>Urządzenie UTM musi umożliwiać łączenie się serwera opisanego w Zadaniu 1 z chmurą.</p> <p>Urządzenie UTM musi współpracować z oprogramowaniem do zarządzania logami opisanym w Zadaniu 8.</p>
24	Procedura odbioru	<p>Procedura odbioru musi być przeprowadzona zgodnie z poniższym opisem:</p> <p>1. W każdym etapie procedury odbioru przedmiotu zamówienia, od weryfikacji dostawy po testy funkcjonalne obowiązkowy jest udział przedstawiciela dostawcy. Rola przedstawiciela wykonawcy obejmuje:</p> <ul style="list-style-type: none"> • udzielanie wsparcia technicznego, w tym wyjaśnień dotyczących funkcji, konfiguracji i możliwości urządzeń, • aktywne uczestnictwo w planowaniu i realizacji testów funkcjonalnych oraz zintegrowanych, zapewniające, że wszystkie aspekty techniczne są prawidłowo zaimplementowane, • natychmiastowe reagowanie na wszelkie problemy techniczne czy niezgodności wykryte podczas testów, oferowanie rozwiązań lub rekomendacji zmian. <p>Zamawiający dopuszcza udział zdalny dostawcy.</p> <p>2. Przyjęcie urządzeń i sprawdzenie kompletności dostawy. Wszystkie komponenty, akcesoria i dokumentacja techniczna muszą być zgodne z umową.</p> <p>3. Sporządzenie protokołu przyjęcia, który dokumentuje stan dostawy, numer seryjny urządzenia oraz wszelkie niezgodności.</p> <p>4. Sprawdzenie zgodności dostarczonej dokumentacji z umową.</p> <p>5. Przeprowadzenie serii testów mających na celu sprawdzenie, czy urządzenie wykonuje wszystkie funkcje określone w specyfikacji technicznej:</p> <ul style="list-style-type: none"> • dla każdej funkcji opisanej w opisie przedmiotu zamówienia zostaną wykonane testy, operacje lub sprawdzenie funkcjonalności urządzeń mające na celu stwierdzenie zgodności z wymogami opisu przedmiotu zamówienia, • każdy test będzie udokumentowany, w tym opis

		<p>procedury, wykonane kroki, uzyskane wyniki oraz wszelkie nieprawidłowości czy odchylenia od oczekiwanych rezultatów,</p> <ul style="list-style-type: none"> • wszystkie zebrane dane zostaną poddane analizie, aby ocenić, czy urządzenie spełnia wymagane specyfikacje, • sporządzanie szczegółowego raportu z testów, zawierającego wnioski oraz wszelkie zidentyfikowane problemy i propozycje ich rozwiązania. <p>6. Sporządzenie szczegółowego protokołu odbioru, który zawiera wyniki wszystkich testów, obserwacje dotyczące stanu urządzenia, i potwierdzenie zgodności z wymaganiami umowy.</p> <p>7. Po pozytywnym zakończeniu testów i potwierdzeniu przez zamawiającego spełnienia wszystkich warunków umowy, zamawiający wydaje formalne potwierdzenie dokonania odbioru przedmiotu umowy.</p>
--	--	--

3.5 Zadanie 5: Wielofunkcyjne źródło zasilania

L.p.	Wymaganie	Opis wymagania
1	Cel	Celem zamówienia jest zakup wielofunkcyjnego źródła zasilania awaryjnego o wysokiej pojemności i mocy, które zapewni nieprzerwaną pracę urządzeń kluczowych dla funkcjonowania Urzędu Miejskiego w Białym Borze podczas przerw w dostawie energii elektrycznej.
2	Moc wyjściowa AC	Urządzenie musi posiadać moc znamionową nie mniejszą niż 2000 W, z możliwością obsługi krótkotrwałych skoków mocy do 3500 W.
3	Pojemność akumulatora	Pojemność baterii urządzenia nie może być mniejsza niż 3000 Wh.
4	Cykl życia baterii	Liczba cykli ładowania musi wynosić co najmniej 500 przy 80% pojemności.
5	Wejście AC	Urządzenie musi posiadać wejście sieciowe AC kompatybilne z polską siecią energetyczną o napięciu 230V oraz częstotliwości 50 Hz.
6	Wyjścia AC	Urządzenie musi posiadać co najmniej dwa gniazda AC 230V.
7	Zakres temperatury pracy	Urządzenie musi pracować w zakresie temperatur co najmniej od 10°C do 36°C.
8	Możliwość ładowania	Urządzenie musi obsługiwać ładowanie z sieci energetycznej.
9	Zabezpieczenia	Urządzenie musi być wyposażone w system zarządzania baterią (BMS) zapewniający ochronę

		przed przeładowaniem, nadmiernym rozładowaniem i przegrzaniem.
10	Porty USB	Urządzenie musi posiadać co najmniej dwa porty USB-C o mocy minimum 60W oraz dwa porty USB-A o mocy co najmniej 12W.
11	Gwarancja	Gwarancja musi obejmować okres 24 miesięcy od dnia podpisania protokołu odbioru.
12	Skalowalność	Urządzenie powinno umożliwiać rozszerzenie pojemności baterii poprzez moduły rozszerzające.
13	Wymagania dotyczące kompatybilności	Urządzenie musi być kompatybilne i umożliwić awaryjne zasilanie urządzeń opisanych w zadaniu 6 (w tym urządzeń sieciowych takich jak przełączniki, serwery, urządzenia UTM itp.), a także zapewnić możliwość awaryjnego podtrzymania pracy wybranych systemów w celu zapewnienia ciągłości działania usług IT w przypadku braku zasilania z sieci energetycznej.
14	Komunikacja	Urządzenie musi posiadać możliwość monitorowania pracy oraz sterowania (np. z poziomu aplikacji mobilnej dla systemów Android, poprzez Bluetooth lub Wi-Fi).

3.6 Zadanie 6: Przełączniki sieciowe

Przełącznik 24 portowy – 1 sztuka

L.p.	Wymaganie	Opis wymagania
1	Typ obudowy	Urządzenie musi być przeznaczone do montażu w szafie RACK 19" i być dostarczone z kompletem akcesoriów montażowych (śruby mocujące itp.).
2	Ilość sztuk	1
3	Liczba portów	Urządzenie musi posiadać co najmniej 24 porty Ethernet 10/100/1000 Mb/s oraz 2 porty SFP 1000 Mb/s.
4	Zarządzanie	Przełącznik musi być zarządzalny na poziomie <u>L3</u> i obsługiwać interfejs zarządzania przez przeglądarkę WWW (GUI).
5	Power over Ethernet (PoE)	Urządzenie musi obsługiwać standardy PoE IEEE 802.3af oraz PoE+ IEEE 802.3at.
6	Obsługiwane protokoły	Przełącznik musi obsługiwać standardy sieciowe, w tym IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE

		802.3z, IEEE 802.1Q (VLAN), IEEE 802.1p (QoS), IEEE 802.1w (RSTP), IEEE 802.3x (flow control).
7	VLAN	Urządzenie musi obsługiwać VLAN.
8	Jakość usług (QoS)	Urządzenie musi obsługiwać funkcje QoS, w tym klasyfikację ruchu na poziomie L2/L3/L4 oraz priorytetyzację pakietów.
9	Mechanizmy zabezpieczeń	Przełącznik musi obsługiwać mechanizmy bezpieczeństwa, takie jak izolacja portów, autoryzacja IEEE 802.1x.
10	Zasilanie	Urządzenie musi być kompatybilne z siecią elektroenergetyczną o napięciu 230V ±10% oraz częstotliwości 50 Hz.
11	Temperatura pracy	Urządzenie musi pracować w zakresie temperatur co najmniej od 10°C do +36°C. Zamawiający dopuszcza urządzenia pracujące w szerszym zakresie.
12	Kompatybilność z systemem backupu i wymagania sieciowe	Urządzenie musi zapewniać przepustowość i liczbę portów wystarczającą do obsługi procesu backupu serwera zgodnie z opisem w zadaniu 1, w tym ruchu pomiędzy serwerem a urządzeniem magazynującym dane. Urządzenie musi gwarantować stabilne działanie w warunkach przewidzianych przez Zamawiającego, uwzględniając typowe scenariusze przesyłania danych (np. pełne i przyrostowe kopie, harmonogram nocny, przepływ w jedną lub obie strony).
13	Gwarancja	Minimalny okres gwarancji na urządzenie musi wynosić 24 miesiące, liczony od dnia podpisania protokołu odbioru przedmiotu zamówienia. Wykonawca musi zapewniać maksymalny czas naprawy lub wymiany urządzenia nie dłuższy niż 14 dni roboczych.

Przełączniki 16 portowe – 2 szt.

L.p.	Wymaganie	Opis wymagania
1	Typ obudowy	Urządzenie musi być przeznaczone do montażu w szafie RACK 19".
2	Ilość sztuk	2
3	Liczba portów	Urządzenie musi posiadać co najmniej 16 portów Ethernet 10/100/1000 Mb/s oraz 2 porty SFP

		1000 Mb/s.
4	Zarządzanie	Przełącznik musi być zarządzalny na poziomie L2 i obsługiwać interfejs zarządzania przez przeglądarkę WWW (GUI).
5	Power over Ethernet (PoE)	Urządzenie musi obsługiwać standardy PoE IEEE 802.3af oraz PoE+ IEEE 802.3at.
6	Obsługiwane standardy	Przełącznik musi obsługiwać standardy sieciowe, w tym IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.1Q (VLAN), IEEE 802.1p (QoS), IEEE 802.3x (flow control).
7	Jakość usług (QoS)	Urządzenie musi obsługiwać funkcje QoS, w tym klasyfikację ruchu na poziomie L2 oraz priorytetyzację pakietów.
8	Mechanizmy zabezpieczeń	Przełącznik musi obsługiwać mechanizmy bezpieczeństwa, takie jak izolacja portów, autoryzacja IEEE 802.1x oraz kontrola burzy.
9	Kompatybilność z polską siecią energetyczną	Urządzenie musi być kompatybilne z polską siecią elektroenergetyczną o napięciu 230V oraz częstotliwości 50 Hz.
10	Zdolność przełączania	Przepustowość przełącznika musi wynosić co najmniej 18 Gb/s, a szybkość przekazywania pakietów co najmniej 23,8 Mpps.
11	Ramki Jumbo	Urządzenie musi obsługiwać ramki Jumbo o wielkości co najmniej 9 000 bajtów.
12	Mechanizmy redundancji	Urządzenie musi obsługiwać protokoły Spanning Tree Protocol (STP, RSTP) oraz agregację łączy.
13	Temperatura pracy	Urządzenie musi pracować w zakresie temperatur co najmniej od 10°C do +36°C. Zamawiający dopuszcza urządzenia pracujące w szerszym zakresie.
14	Gwarancja	Minimalny okres gwarancji na urządzenie musi wynosić 24 miesiące liczony od dnia podpisania protokołu odbioru przedmiotu zamówienia.

Przełączniki 8 portowe – 3 szt.

L.p.	Wymaganie	Opis wymagania
1	Typ obudowy	Urządzenie musi być przystosowane do montażu w szafie RACK.
2	Ilość sztuk	3
3	Zarządzanie	Urządzenie musi być zarządzalne na poziomie warstwy L2 oraz umożliwiać zarządzanie przez interfejs WWW (GUI), wiersz poleceń (CLI).

4	Liczba portów Ethernet	Urządzenie musi posiadać co najmniej 8 portów RJ-45 10/100/1000 Mbps.
5	Porty PoE	Urządzenie musi obsługiwać standard PoE+ IEEE 802.3at.
6	Standardy sieciowe	Urządzenie musi obsługiwać standardy IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3af, IEEE 802.3at.
7	Przepustowość	Minimalna przepustowość urządzenia musi wynosić 16 Gb/s.
8	Bufor pamięci	Urządzenie musi posiadać bufor pamięci o minimalnej pojemności minimum 256 KB lub równoważna architektura zapewniająca płynność ruchu przy pełnym obciążeniu portów.
9	Akcesoria	W zestawie musi znajdować się kabel zasilający oraz elementy montażowe do szafy RACK (jeśli dotyczy).
10	Gwarancja	Urządzenie musi posiadać minimalną gwarancję producenta wynoszącą 24 miesiące liczony od dnia podpisania protokołu odbioru przedmiotu zamówienia.

3.7 Zadanie 7: Zakup serwera fizycznego oraz systemu Windows Server lub równoważnego wraz z wdrożeniem i konfiguracją

3.7.1 Serwer

L.p.	Wymaganie	Opis wymagania
1	Cel	<p>Serwer będzie pełnił kluczową rolę w zarządzaniu infrastrukturą IT zamawiającego. Jego główne zastosowania obejmują:</p> <ol style="list-style-type: none"> Zarządzanie tożsamościami i dostępem: serwer zostanie wykorzystany do centralnego zarządzania kontami użytkowników, ich hasłami oraz uprawnieniami dostępu do zasobów sieciowych. Realizacja polityki tworzenia kopii zapasowych: na serwerze może zostać zainstalowane oprogramowanie do

		wykonywania kopii zapasowych zgodnie z wymaganiami określonymi w Zadaniu 2. System backupu umożliwi zabezpieczenie kluczowych danych organizacji, ich szybkie odtworzenie w przypadku awarii oraz zwiększy odporność infrastruktury IT na utratę informacji.
2	Możliwość uruchomienia systemów dziedzinowych wykorzystywanych przez zamawiającego	<p>Dostarczony serwer, musi umożliwiać jednoczesne, stabilne i wydajne uruchomienie następujących systemów w środowisku wirtualizacji:</p> <p>1) eKancelaria (działający w systemie operacyjnym Linux), wymagający min. 8 vCPU, 16 GB RAM, 1 TB przestrzeni dyskowej (zajętość ok. 600 GB),</p> <p>2) GMINA (działający w systemie operacyjnym Linux), wymagający min. 8 vCPU, 16 GB RAM, 1 TB przestrzeni dyskowej (zajętość ok. 50 GB),</p> <p>3) System operacyjny opisany w punkcie 3.7.2 . Minimalne wymagania: 2 vCPU, 8 GB RAM, 200 GB przestrzeni dyskowej,</p> <p>4) GOMIK, KadryPłace, BESTIA, Winsarcz – (aplikacje obecnie działające w systemie operacyjnym Windows) działające łącznie w jednej maszynie wirtualnej wymagającej min. 16 vCPU, 64 GB RAM, 2 TB przestrzeni dyskowej.</p> <p>Dostarczony serwer musi posiadać odpowiednią moc obliczeniową, ilość pamięci RAM oraz przestrzeń dyskową, pozwalającą na jednoczesne funkcjonowanie wszystkich ww. maszyn wirtualnych oraz infrastruktury wirtualizacyjnej, z odpowiednim zapasem na potrzeby systemu backupu oraz rezerwę wydajnościową.</p>
3	Typ obudowy	Urządzenie przystosowane do montażu w szafie RACK o wysokości maksymalnie 2U (dopuszcza się zarówno serwery 1U, jak i 2U).
4	Procesor	Procesor musi być zgodny z systemami operacyjnymi klasy serwerowej (w tym systemem operacyjnym oferowanym w niniejszym postępowaniu) oraz wspierać platformy wirtualizacyjne (oferowane w niniejszym postępowaniu).
5	Liczba rdzeni procesora	Minimum 16 rdzeni.

6	Liczba wątków	Minimum 32 wątków.
7	Pamięć RAM	Zainstalowana pamięć operacyjna minimum 128 GB, rozszerzalna do minimum 1 TB.
8	Dyski twarde	<p>Serwer musi być wyposażony w 10 (dziesięć) dysków półprzewodnikowych SSD klasy enterprise o pojemności nominalnej każdego dysku minimum 960 GB, dopuszcza się także dyski o pojemności do 1,2 TB. Dyski muszą być typu Hot Swap, tj. umożliwiać ich wymianę bez konieczności wyłączania serwera. Łączna pojemność brutto wszystkich dysków musi wynosić co najmniej 8 TB.</p> <p>Dyski mają umożliwiać skonfigurowanie sprzętowej macierzy RAID (np. RAID 1, RAID 5 lub RAID 10) w sposób zapewniający redundancję danych oraz wysoką wydajność pracy serwera.</p>
9	Obsługa RAID	Wbudowany kontroler RAID z obsługą RAID 0, 1, 5, 10.
10	Porty sieciowe	Minimum 2 porty 10/100/1000 Mbps Ethernet RJ-45. Zamawiający dopuszcza zastosowanie adaptera sieciowego.
11	Interfejsy	Minimum 2 porty USB 2.0 lub nowsze oraz 1 port USB 3.2 Gen 1.
12	Moduł zarządzania	Wbudowany moduł zarządzania umożliwiający monitorowanie stanu sprzętu, konfigurację zdalną oraz aktualizacje oprogramowania.
13	Liczba kieszeni na dyski	Minimum 10 zatok na dyski 3,5" lub 2,5".
14	Obsługa Hot-Swap	Możliwość wymiany dysków i zasilaczy podczas pracy systemu.
15	Środowisko pracy	Zakres temperatury pracy co najmniej od 10°C do 35°C. Zamawiający dopuszcza urządzenia pracujące w szerszym zakresie.
16	Wdrożenie	<p>Wykonawca zobowiązany jest do przeprowadzenia pełnego wdrożenia dostarczonego serwera w infrastrukturze Zamawiającego, obejmującego:</p> <ol style="list-style-type: none"> 1. Dostawę, montaż i uruchomienie urządzenia w szafie RACK w lokalizacji wskazanej przez Zamawiającego, 2. Podłączenie urządzenia do infrastruktury zasilającej oraz sieciowej,

		<ol style="list-style-type: none"> 3. Weryfikację poprawności działania sprzętu (testy POST, sprawdzenie dysków, pamięci, interfejsów), 4. Aktualizację firmware i oprogramowania zarządzającego serwerem do najnowszych wersji zalecanych przez producenta, 5. Przeprowadzenie testów sprzętowych celem potwierdzenia pełnej sprawności urządzenia, 6. Przeprowadzenie testów kompatybilności z oprogramowaniem wskazanym w opisie zamówienia (w tym Płatnik, BESTI@).
17	Gwarancja	<ol style="list-style-type: none"> 1. Dostarczony serwer musi być objęty gwarancją przez okres 36 miesięcy, liczony od daty podpisania protokołu odbioru. 2. W ramach gwarancji Wykonawca zapewnia serwis w siedzibie zamawiającego, obejmujący naprawę lub wymianę urządzenia na sprawne. Maksymalny czas na usunięcie awarii wynosi 24 godziny, liczone od momentu zgłoszenia awarii przez Zamawiającego. 3. Zgłoszenie awarii może nastąpić poprzez: <ol style="list-style-type: none"> a. e-mail wysłany na adres serwisowy wskazany przez Wykonawcę, b. aplikację/webowy portal serwisowy udostępniony przez Wykonawcę. 4. Potwierdzenie przyjęcia zgłoszenia przez Wykonawcę musi nastąpić nie później niż w ciągu 4 godzin od chwili otrzymania zgłoszenia (e-mailem lub w aplikacji). W ramach potwierdzenia Wykonawca przekazuje Zamawiającemu: <ol style="list-style-type: none"> a. datę i godzinę przyjęcia zgłoszenia, b. unikalny identyfikator zgłoszenia pozwalający na śledzenie postępu, c. przewidywany termin zakończenia naprawy. 5. Jeżeli Wykonawca nie potwierdzi przyjęcia zgłoszenia w ww. terminie 4 godzin, wówczas 24-godzinny czas na usunięcie awarii liczony jest od momentu wysłania zgłoszenia awarii

		<p>przez Zamawiającego (tj. data i godzina wysłania e-maila lub odnotowania zgłoszenia w aplikacji/portalu).</p> <p>6. W przypadku uszkodzenia dysków twardych, Zamawiający wymaga pozostawienia ich w swojej siedzibie (dyski nie podlegają zwrotowi do Wykonawcy).</p> <p>7. Cała komunikacja z zespołem serwisowym (w tym zgłaszanie awarii, potwierdzenia, informacje o statusie naprawy) odbywa się w języku polskim.</p> <p>W ramach gwarancji producent lub dostawca sprzętu musi zapewnić:</p> <p>1. Dostęp do najnowszych aktualizacji oprogramowania, związanego ze sprzętem, które mają na celu utrzymanie oprogramowania w pełni funkcjonalnym, muszą obejmować poprawki bezpieczeństwa, aktualizacje kompatybilności z dostarczonymi systemami operacyjnymi oraz dostarczonym oprogramowaniem do backupu, jak również wszelkie usprawnienia funkcjonalne i optymalizacyjne dostarczane przez producenta oprogramowania mające na celu zapewnienie bezpieczeństwa oprogramowania, w przypadku ujawnienia podatności bezpieczeństwa (np. CVE) w dostarczonym oprogramowaniu związanym ze sprzętem, celem usunięcia tych podatności i uzyskania oprogramowania wolnego od podatności bezpieczeństwa.</p> <p>2. Wszystkie aktualizacje muszą być dostarczane bez dodatkowych kosztów dla Zamawiającego, a procedury ich wdrażania muszą być jasno opisane w dokumentacji technicznej.</p>
--	--	--

3.7.2 System operacyjny

L.p.	Wymaganie	Opis wymagania
------	-----------	----------------

1	Dostawa systemu operacyjnego	<p>Wykonawca zobowiązany jest do dostawy systemu operacyjnego umożliwiającego zarządzanie serwerem, klasy równoważnej do Microsoft Windows Server w najnowszej wersji dostępnej u producenta na dzień składania ofert.</p> <p>Parametry równoważności opisano w punktach od 5 do 22</p> <p>Dostarczony system operacyjny musi umożliwiać działanie oprogramowania wykorzystywanego przez zamawiającego BESTI@ oraz Płatnik z uwagi na konieczność zapewnienia ciągłości kluczowych zadań urzędu, instalacja tych aplikacji na dostarczonym systemie operacyjnym umożliwi lepszą kontrolę dostępu, tworzenie kopii zapasowych danych finansowych i kadrowych, a także podniesie odporność na błędy i awarie.</p>
2	Zapewnienie działania wskazanych systemów w środowisku wirtualnym	<p>Wykonawca zobowiązany jest do dostarczenia i skonfigurowania systemu operacyjnego wraz z mechanizmem wirtualizacji, w sposób umożliwiający stabilne, wydajne i jednocześnie działanie wskazanych przez Zamawiającego systemów:</p> <ol style="list-style-type: none"> 1) eKancelaria (obecnie działający na systemie operacyjnym Linux), 2) GMINA (obecnie działający na systemie operacyjnym Linux), 3) Usługa katalogowa umożliwiająca centralne zarządzanie tożsamościami i zasobami w sieci komputerowej. Wymagania minimalne: 2 vCPU, 8 GB RAM, 200 GB dysk, 4) GOMIK, KadryPłace, BESTIA, Winsarcz (obecnie działający na systemie operacyjnym Windows). <p>System operacyjny musi zawierać mechanizmy wirtualizacji, które umożliwiają tworzenie maszyn wirtualnych oraz zarządzanie nimi. Środowisko musi zapewniać odpowiednią moc obliczeniową, zasoby pamięci operacyjnej i przestrzeni dyskowej dla ww. maszyn, a także gwarantować ich poprawną i wydajną pracę.</p> <p>Dostarczone rozwiązanie musi zostać przetestowane pod kątem uruchomienia i działania wymienionych</p>

		<p>systemów. Wykonawca jest zobowiązany do zapewnienia, że wszystkie wskazane systemy zostaną uruchomione i będą działać w pełni funkcjonalnie na dostarczonym serwerze oraz systemie operacyjnym w ramach środowiska wirtualnego.</p> <p>W razie problemów z uruchomieniem któregokolwiek z ww. systemów, Wykonawca zobowiązuje się do nieodpłatnej modyfikacji konfiguracji lub dostarczenia dodatkowych komponentów w celu zapewnienia zgodności i działania.</p>
3	Licencje dostępowe	Licencje dostępowe muszą umożliwiać 25 użytkownikom jednocześnie korzystanie z usług dostarczonego systemu operacyjnego, w tym usług katalogowych i sieciowych.
4	Kryteria równoważności	W przypadku zaoferowania systemu równoważnego, musi on spełniać wszystkie poniżej określone wymagania funkcjonalne – punkty od 5 do 22 niniejszej tabeli.
5	Środowisko fizyczne i wirtualne	Licencja musi umożliwiać uruchamianie systemu operacyjnego w środowisku fizycznym oraz w co najmniej dwóch wirtualnych środowiskach.
6	Wymagania dla środowiska wirtualnego	Każdy wirtualny system musi obsługiwać co najmniej 64 procesory wirtualne, 1 TB RAM i dyski o pojemności co najmniej 64 TB.
7	Migracja maszyn wirtualnych	Możliwość migracji maszyn wirtualnych pomiędzy serwerami bez przerywania pracy, przez sieć Ethernet, bez mechanizmów współdzielenia pamięci.
8	Hot swap pamięci RAM	System musi wspierać funkcję dodawania i wymiany pamięci RAM bez przerywania pracy (na sprzęcie obsługującym tę funkcjonalność).
9	Hot swap procesorów	System musi wspierać funkcję dodawania i wymiany procesorów bez przerywania pracy (na sprzęcie obsługującym tę funkcjonalność).
10	Weryfikacja sterowników	Automatyczna weryfikacja cyfrowych sygnatur sterowników zapewniająca ich sprawdzenie przez producenta systemu.
11	Zarządzanie energią	Dynamiczne obniżanie poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
12	Klasyfikacja plików	Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
13	Obsługa ASP.NET	Wsparcie dla uruchamiania aplikacji internetowych

		wykorzystujących technologię ASP.NET.
14	Dystrybucja ruchu sieciowego	Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
15	Firewall	Wbudowana zaporą sieciową (firewall) z możliwością definiowania reguł ochrony dla połączeń internetowych i intranetowych.
16	Lokalizacja systemu	Interfejs użytkownika, przeglądarka, pomoc i komunikaty systemowe muszą być dostępne w języku polskim.
17	Zmiana języka	Możliwość zmiany języka interfejsu systemowego po instalacji, dla co najmniej dwóch języków.
18	Obsługa urządzeń peryferyjnych	Wsparcie dla powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, USB, Plug & Play).
19	Zdalna administracja	Możliwość zdalnej konfiguracji, administracji oraz aktualizacji systemu.
20	Multipath I/O	Wsparcie dla dostępu do zasobów dyskowych poprzez mechanizm Multipath I/O.
21	Instalacja poprawek	Możliwość instalacji poprawek poprzez ich integrację z obrazem instalacyjnym systemu.
22	Administracja skryptowa	Wbudowane mechanizmy zdalnej administracji oraz administracji skryptowej.
23	Wdrożenie	<p>System operacyjny, o którym mowa w powyższych punktach (1–22), musi umożliwiać wdrożenie usługi katalogowej zapewniającej:</p> <ol style="list-style-type: none"> 1. Centralne zarządzanie kontami użytkowników i urządzeniami, 2. Zarządzanie uprawnieniami, w tym nadawanie i odbieranie dostępu do zasobów sieciowych (np. dysków sieciowych, drukarek), 3. Realizację polityk bezpieczeństwa – w szczególności wymuszanie minimalnej złożoności haseł, okresowej ich zmiany oraz blokady kont w przypadku nieuprawnionego dostępu, 4. Obsługę uwierzytelniania w standardzie LDAP lub równoważnym (np. celem integracji z innymi usługami sieciowymi), 5. Centralną dystrybucję ustawień stacji roboczych, w tym możliwość tworzenia reguł i zasad konfiguracyjnych dla komputerów oraz użytkowników, 6. Współpracę z oprogramowaniem stosowanym

		<p>w Urzędzie (np. systemami dziedzinowymi i rozwiązaniami do backupu),</p> <p>7. Możliwość integracji z usługami wirtualizacji wdrożonymi w ramach niniejszego zamówienia (o ile zostaną utworzone środowiska wirtualne).</p> <p>W ramach prac wdrożeniowych Wykonawca zobowiązany jest do:</p> <ul style="list-style-type: none"> • Instalacji i konfiguracji usługi katalogowej na dostarczonym serwerze, • Opracowania struktury i grup użytkowników w sposób odzwierciedlający potrzeby Zamawiającego, • Migracji lub założenia kont użytkowników zgodnie z wytycznymi Zamawiającego, • Konfiguracji polityk bezpieczeństwa (m.in. w zakresie haseł i dostępu do zasobów), • Przeszkolenia pracowników odpowiedzialnych za administrowanie systemem w podstawowym zakresie obsługi usługi katalogowej (np. tworzenie i zarządzanie kontami, wdrażanie nowych polityk).
--	--	--

3.8 Zadanie 8: Zlecenie instalacji, konfiguracji i wsparcia technicznego oprogramowania OpenSource do zarządzania logami

L.p.	Wymaganie	Opis wymagania
1	Cel	<p>Celem zakupu i wdrożenia systemu do zarządzania logami jest zwiększenie poziomu bezpieczeństwa informatycznego oraz usprawnienie monitorowania i analizy zdarzeń w infrastrukturze IT zamawiającego. Centralizacja logów oraz wdrożenie mechanizmów raportowania i alertowania pozwolą na szybsze wykrywanie incydentów oraz lepsze zarządzanie danymi operacyjnymi i bezpieczeństwa. Zamawiający przewiduje również realizację szkolenia dla pracowników IT w zakresie obsługi</p>

		wdrożonego systemu logów, zgodnie z Zadaniem 11.
2	Instalacja i konfiguracja oprogramowania	Wykonawca zainstaluje i skonfiguruje w środowisku zamawiającego oprogramowanie do zarządzania logami, np. Graylog (np. open-source, licencja SSPL). Instalacja obejmie wszystkie niezbędne komponenty (np.: system operacyjny, silniki, bazę danych, silnik wyszukiwania itp.) oraz dostosowanie konfiguracji do środowiska zamawiającego. Oprogramowanie do zarządzania logami wykonawca musi zainstalować na serwerze opisanym w Zadaniu 9.
3	Integracja z infrastrukturą organizacji	Wykonawca podłączy i skonfiguruje źródła logów z istniejącej infrastruktury zamawiającego do centralnego systemu do zarządzania logami. Obejmuje to logi systemowe z serwerów aplikacji w tym Windows i Linux, logi z urządzeń sieciowych (np. UTM, przełączników), systemów backupu, aplikacji wykorzystywanych przez urząd (np. Gmina 3, eKancelaria), a także innych istotnych komponentów infrastruktury informatycznej wskazanych przez Zamawiającego. Konfiguracja musi obejmować mechanizmy transportu logów (np. Syslog, lub inne).
4	Wdrożenie funkcjonalności raportowania, alertów i dashboardów	Wykonawca wdroży funkcjonalności, takie jak dashboardy z wizualizacją metryk i statystyk (np. liczba zdarzeń, statusy usług, alerty bezpieczeństwa). Skonfiguruje alerty e-mailowe w reakcji na określone zdarzenia oraz opracuje szablony raportów okresowych i na żądanie, podsumowujących incydenty i statystyki wykorzystania systemów. Wszystkie funkcje będą dostępne dla uprawnionych użytkowników poprzez interfejs oprogramowania.
5	Wymagania dotyczące kompatybilności i integracji	Oprogramowanie musi współpracować i integrować się z serwerem opisanym w zadaniu 1 oraz oprogramowaniem opisanym w zadaniu 2.
6	Świadczenie podstawowej pomocy technicznej	Wykonawca zapewni wsparcie techniczne przez okres 8 miesięcy, nie dłużej niż do 30.04.2026, obejmujące pomoc w rozwiązywaniu problemów, konsultacje dotyczące aktualizacji i konfiguracji oraz ogólną asystę w utrzymaniu systemu.

Wsparcie techniczne musi obejmować:

- pomoc w rozwiązywaniu bieżących problemów technicznych związanych z funkcjonowaniem oprogramowania do zarządzania logami,
- konsultacje dotyczące aktualizacji systemu oraz jego konfiguracji,
- zdalne rozwiązywanie incydentów (poprzez e-mail, telefon lub inne uzgodnione kanały),
- sprawdzanie poprawności działania systemu i rekomendowanie ewentualnych usprawnień,
- odpowiedzi na pytania i problemy zgłaszane przez administratorów systemu po stronie zamawiającego.

Czas reakcji na zgłoszenie nie może przekroczyć **8 godzin roboczych**, a czas usunięcia problemu nie może przekroczyć 24 godzin roboczych, o ile nie zachodzą okoliczności niezależne od wykonawcy (np. awarie niezależnych komponentów systemu). W takim przypadku wykonawca niezwłocznie poinformuje Zamawiającego i przedstawi harmonogram działań naprawczych.

Wszelkie działania wsparcia świadczone są bez dodatkowych kosztów dla Zamawiającego.

3.9 Zadanie 9: Zakup serwera na potrzeby oprogramowania do zarządzania logami oraz do zarządzania infrastrukturą IT wraz z niezbędnym oprogramowaniem systemowym

L.p.	Wymaganie	Opis wymagania
1	Cel	Celem zakupu serwera jest zapewnienie platformy niezbędnej do uruchomienia oprogramowania opisanego w Zadaniu 8. Dzięki temu możliwe będzie centralne gromadzenie i przetwarzanie logów z różnych elementów środowiska (serwerów, urządzeń sieciowych, aplikacji itp.), co umożliwi szybką analizę zdarzeń, sprawniejsze wykrywanie incydentów bezpieczeństwa oraz usprawni proces raportowania i alertowania.
2	Typ obudowy	Urządzenie przystosowane do montażu w szafie RACK o wysokości maksymalnie 2U (dopuszcza się zarówno serwery 1U, jak i 2U).
3	Procesor	Procesor musi być przeznaczony do pracy w serwerach i systemach klasy enterprise. Musi być przystosowany do obsługi technologii wirtualizacji
4	Liczba rdzeni procesora	Minimum 16 rdzeni.
5	Liczba wątków	Minimum 32 wątków.
6	Pamięć RAM	Zainstalowana pamięć operacyjna minimum 64 GB, rozszerzalna do minimum 1 TB.
7	Dyski twarde	Co najmniej 2 dyski SSD o pojemności 4TB każdy, z możliwością konfiguracji RAID.
8	Obsługa RAID	Wbudowany kontroler RAID z obsługą RAID 0, 1, 5, 10.
9	Porty sieciowe	Minimum 2 porty 10/100/1000 Mbps Ethernet RJ-45.
10	Interfejsy	Minimum 2 porty USB 2.0 lub nowsze oraz 1 port USB 3.2 Gen 1.
11	Moduł zarządzania	Wbudowany moduł zarządzania umożliwiający monitorowanie stanu sprzętu, konfigurację zdalną oraz aktualizacje oprogramowania.

12	Liczba kieszeni na dyski	Minimum 8 zatok na dyski 3,5" lub 2,5".
13	Obsługa Hot-Swap	Możliwość wymiany dysków i zasilaczy podczas pracy systemu.
14	Środowisko pracy	Zakres temperatury pracy od 10°C do 35°C.
15	System operacyjny	W ramach przedmiotu zamówienia Wykonawca dostarczy i zainstaluje system operacyjny, zgodny z wymaganiami oprogramowania opisanego w Zadaniu 8 oraz Zadaniu 10. System operacyjny musi być stabilny, wspierany przez społeczność lub producenta przez co najmniej 3 lata od daty instalacji i umożliwiać aktualizacje związane z bezpieczeństwem.
16	Dostawa	Wykonawca musi dostarczyć oraz uruchomić serwer w infrastrukturze IT Zamawiającego. Proces ten obejmuje montaż serwera w szafie RACK, podłączenie do zasilania i sieci LAN, wstępną konfigurację systemu operacyjnego oraz uruchomienie podstawowych usług sieciowych niezbędnych do dalszej instalacji oprogramowania wskazanego w Zadaniu 8.
17	Gwarancja	<p>8. Dostarczony serwer musi być objęty gwarancją przez okres 36 miesięcy, liczony od daty podpisania protokołu odbioru.</p> <p>9. W ramach gwarancji Wykonawca zapewnia serwis w siedzibie zamawiającego, obejmujący naprawę lub wymianę urządzenia na sprawne. Maksymalny czas na usunięcie awarii wynosi 24 godziny, liczone od momentu zgłoszenia awarii przez Zamawiającego.</p> <p>10. Zgłoszenie awarii może nastąpić poprzez:</p> <ul style="list-style-type: none"> a. e-mail wysłany na adres serwisowy wskazany przez Wykonawcę, b. aplikację/webowy portal serwisowy udostępniony przez Wykonawcę. <p>11. Potwierdzenie przyjęcia zgłoszenia przez Wykonawcę musi nastąpić nie później niż w ciągu 4 godzin od chwili otrzymania zgłoszenia (e-mailem lub w aplikacji). W ramach potwierdzenia Wykonawca przekazuje</p>

	<p>Zamawiającemu:</p> <ol style="list-style-type: none">datę i godzinę przyjęcia zgłoszenia,unikalny identyfikator zgłoszenia pozwalający na śledzenie postępu,przewidywany termin zakończenia naprawy. <p>12. Jeżeli Wykonawca nie potwierdzi przyjęcia zgłoszenia w ww. terminie 4 godzin, wówczas 24-godzinny czas na usunięcie awarii liczony jest od momentu wysłania zgłoszenia awarii przez Zamawiającego (tj. data i godzina wysłania e-maila lub odnotowania zgłoszenia w aplikacji/portalu).</p> <p>13. W przypadku uszkodzenia dysków twardych, Zamawiający wymaga pozostawienia ich w swojej siedzibie (dyski nie podlegają zwrotowi do Wykonawcy).</p> <p>14. Cała komunikacja z zespołem serwisowym (w tym zgłaszanie awarii, potwierdzenia, informacje o statusie naprawy) odbywa się w języku polskim.</p> <p>W ramach gwarancji producent lub dostawca sprzętu musi zapewnić:</p> <ol style="list-style-type: none">Dostęp do najnowszych aktualizacji oprogramowania, związanego ze sprzętem, które mają na celu utrzymanie oprogramowania w pełni funkcjonalnym, muszą obejmować poprawki bezpieczeństwa, aktualizacje kompatybilności z dostarczonymi systemami operacyjnymi oraz dostarczonym oprogramowaniem do backupu, jak również wszelkie usprawnienia funkcjonalne i optymalizacyjne dostarczane przez producenta oprogramowania mające na celu zapewnienie bezpieczeństwa oprogramowania, w przypadku ujawnienia podatności bezpieczeństwa (np. CVE) w dostarczonym oprogramowaniu związanym ze sprzętem, celem usunięcia tych podatności i
--	---

		<p>uzyskania oprogramowania wolnego od podatności bezpieczeństwa.</p> <p>2. Wszystkie aktualizacje związane z bezpieczeństwem muszą być dostarczane bez dodatkowych kosztów dla Zamawiającego, a procedury ich wdrażania muszą być jasno opisane w dokumentacji technicznej.</p>
--	--	--

3.10 Zadanie 10: Zakup oprogramowania do zarządzania infrastrukturą IT wraz z usługą instalacji i konfiguracji

L.p.	Wymaganie	Opis wymagania
1	Rejestracja zgłoszeń serwisowych (ServiceDesk)	Możliwość rejestrowania incydentów oraz wniosków o usługi IT.
2	Zarządzanie incydentami	Obsługa i monitorowanie incydentów.
3	Zarządzanie problemami	Identyfikacja i analiza przyczyn problemów oraz wdrażanie działań naprawczych.
4	Analiza zgodności z SLA	Monitorowanie i raportowanie zgodności działań z ustalonymi umowami o poziomie usług.
5	Automatyczne przypisywanie zgłoszeń	Reguły umożliwiające automatyczne kierowanie zgłoszeń do odpowiednich zespołów lub osób.
6	Centralna baza konfiguracji (CMDB)	Przechowywanie informacji o komponentach infrastruktury IT i ich relacjach.
7	Budowanie relacji między elementami konfiguracji	Tworzenie powiązań między elementami w CMDB w celu lepszego zarządzania usługami.
8	Automatyczna inwentaryzacja zasobów IT	Systemowe skanowanie i rejestrowanie sprzętu oraz oprogramowania w organizacji.
9	Ewidencja dokumentacji powiązanej z zasobami	Przechowywanie faktur, kart gwarancyjnych i innych dokumentów związanych z zasobami.
10	Zarządzanie cyklem życia	Śledzenie etapów od zakupu, przez

	zasobów	użytkowanie, aż po wycofanie zasobów z eksploatacji.
11	Rejestrowanie konfiguracji sprzętowej	Oprogramowanie musi umożliwiać zbieranie i aktualizowanie informacji o parametrach technicznych komputerów.
12	Ewidencjonowanie zainstalowanego oprogramowania	Oprogramowanie musi pozwalać na monitorowanie i raportowanie używanych aplikacji.
13	Zdalny dostęp i kontrola urządzeń	Oprogramowanie musi umożliwiać administratorowi łączenie się z komputerami użytkowników w celu diagnozy, konfiguracji i rozwiązywania problemów.
14	Kontrola legalności i wykorzystywania licencji	Oprogramowanie musi umożliwiać monitorowanie dostępnych licencji, i przeprowadzanie audytów oprogramowania.
15	Kontrola dostępu do nośników danych USB	Oprogramowanie musi posiadać funkcjonalności ograniczające możliwość używania zewnętrznych pamięci masowych w celu zapobiegania wyciekom danych.
16	Interfejs użytkownika	Możliwość dostosowania interfejsu do indywidualnych potrzeb użytkownika.
17	Reguły sterujące logiką pracy systemu	Definiowanie warunków i akcji automatyzujących procesy w systemie.
18	Instalacja oprogramowania	Wykonawca zainstaluje oprogramowanie zgodnie z wymaganiami zamawiającego, w tym wszystkie niezbędne komponenty oraz zależności systemowe. Ilość stacji komputerowych: 25.
19	Konfiguracja oprogramowania	Wykonawca dostosuje konfigurację systemu zgodnie z wymaganiami zamawiającego, w tym konfigurację użytkowników, reguł bezpieczeństwa oraz dostępu.
20	Integracja z infrastrukturą IT	Wykonawca musi zainstalować, skonfigurować oprogramowanie z istniejącą infrastrukturą IT, w tym systemów monitorowania, baz danych oraz usług katalogowych.
21	Testy wdrożeniowe	Wykonawca przeprowadzi testy poprawności działania systemu po instalacji i konfiguracji.

22	Dokumentacja techniczna	Wykonawca dostarczy pełną dokumentację instalacyjną oraz konfiguracyjną wdrożonego systemu.
23	Licencja	W ramach licencji Zamawiający otrzymuje prawo do korzystania z oprogramowania oraz do wszelkich jego aktualizacji bezpieczeństwa i nowych wydań wydanych w okresie obowiązywania licencji. Licencja obejmuje pełną funkcjonalność wymienioną w punktach 1–23 oraz uprawnia Zamawiającego do instalacji i użytkowania oprogramowania na 25 stanowiskach. W przypadku gdy w ramach licencji wliczona jest subskrypcja to musi ona wynosić 8 miesięcy nie dłużej niż do 30.04.2026 r. od dnia podpisania protokołu odbioru.

3.11 Zadanie 11: Zakup szkolenia dla pracowników obsługi informatycznej z obsługi i użytkowania oprogramowania do analizy logów systemowych

L.p.	Wymaganie	Opis wymagania
1	Szkolenie dla administratora systemu	Wykonawca przeprowadzi dedykowane szkolenie dla jednego pracownika organizacji (informatyka), który będzie pełnił rolę administratora systemu opisanego w zadaniu nr 8. Szkolenie obejmie zarówno podstawowe, jak i zaawansowane funkcje systemu, aby umożliwić samodzielne zarządzanie i utrzymanie systemu.
2	Cel szkolenia	Celem szkolenia jest przygotowanie informatyka do efektywnej administracji systemem, zapewnienia jego optymalnego działania oraz integracji z infrastrukturą IT zamawiającego.
3	Zakres szkolenia – Wstęp	Wprowadzenie do systemu: architektura systemu, rola poszczególnych komponentów,

		podstawowe funkcjonalności.
4	Zakres szkolenia – Instalacja i konfiguracja	Praktyczne omówienie procesu instalacji i konfiguracji oprogramowania na systemie zamawiającego, w tym dostosowanie ustawień systemowych i integracja z bazą danych oraz silnikiem wyszukiwania.
5	Zakres szkolenia – Integracja z infrastrukturą IT	Konfiguracja źródeł logów, transport logów przy użyciu np. Syslog i innych metod, integracja z serwerami Windows Server oraz urządzeniami UTM.
6	Zakres szkolenia – Zarządzanie użytkownikami i uprawnieniami	Tworzenie i zarządzanie kontami użytkowników, przypisywanie ról i uprawnień, konfiguracja dostępu do logów i raportów.
7	Zakres szkolenia – Tworzenie i zarządzanie dashboardami	Konfiguracja kokpitów administracyjnych, tworzenie widżetów wizualizujących dane, optymalizacja wyglądu i użyteczności dashboardów.
8	Zakres szkolenia – System alertów	Definiowanie reguł i warunków uruchamiania alertów, konfiguracja powiadomień e-mailowych i webhooków, monitorowanie krytycznych zdarzeń systemowych.
9	Zakres szkolenia – Raportowanie	Tworzenie szablonów raportów okresowych i niestandardowych, automatyzacja generowania raportów, eksportowanie danych do różnych formatów.
10	Zakres szkolenia – Optymalizacja systemu	Monitorowanie wydajności systemu, analiza zużycia zasobów, strategie optymalizacji działania oprogramowania i powiązanych usług.
11	Zakres szkolenia – Rozwiązywanie problemów	Diagnostyka i usuwanie awarii, analiza błędów i logów systemowych, procedury postępowania w sytuacjach kryzysowych.
12	Forma szkolenia	Szkolenie musi odbyć się w formie warsztatowej, w trybie online, z udziałem prowadzącego na żywo. Uczestnik szkolenia będzie miał dostęp do wdrożonego systemu w środowisku produkcyjnym.
13	Czas trwania szkolenia	Szkolenie będzie trwało jeden dzień (min. 6 godzin szkoleniowych) i obejmie zarówno teorię, jak i ćwiczenia praktyczne.
14	Materiały szkoleniowe	Wykonawca dostarczy materiały szkoleniowe w formie elektronicznej lub papierowej, zawierające instrukcje dotyczące obsługi

		systemu, przykłady konfiguracji oraz procedury zarządzania i utrzymania systemu.
15	Egzamin końcowy / weryfikacja wiedzy	Po zakończeniu szkolenia administrator systemu odbędzie test sprawdzający wiedzę, a wykonawca dostarczy raport podsumowujący jego wyniki oraz zalecenia dotyczące dalszego doskonalenia umiejętności. Wynik testu ma charakter wyłącznie informacyjny i nie wpływa na ocenę wykonania przedmiotu zamówienia.
16	Kontakt po szkoleniu	Wykonawca zapewni możliwość kontaktu (np. drogą mailową lub telefoniczną) w celu konsultacji i wyjaśnienia ewentualnych wątpliwości dotyczących materiału szkoleniowego przez okres 30 dni kalendarzowych po zakończeniu szkolenia.

3.12 Zadanie 12: Zakup szkolenia dla pracowników obsługi informatycznej z obsługi i użytkowania oprogramowania do zarządzania infrastrukturą

L.p.	Wymaganie	Opis wymagania
1	Szkolenie dla administratora systemu	Wykonawca przeprowadzi szkolenie dla jednego pracownika organizacji (informatyka) odpowiedzialnego za administrację systemem. Celem szkolenia jest zapewnienie kompetencji niezbędnych do samodzielnego zarządzania, obsługi i utrzymania wdrożonego systemu.
2	Forma szkolenia	Szkolenie musi zostać przeprowadzone w formie warsztatowej (online), z wykorzystaniem wdrożonego systemu. Szkolenie musi obejmować część praktyczną z wykorzystaniem infrastruktury Zamawiającego.
3	Czas trwania	Szkolenie musi trwać minimum 8 godzin dydaktycznych i zostać zrealizowane w ciągu jednego dnia lub w dwóch sesjach po 4 godziny.
4	Zakres szkolenia – podstawy	Omówienie architektury systemu, funkcjonalności oraz sposobów wykorzystania w codziennej pracy administracyjnej. Praktyczne ćwiczenia z konfiguracji elementów systemu: ServiceDesk, CMDB, monitorowania

		zasobów IT, zarządzania cyklem życia zasobów, raportowania, zarządzania uprawnieniami, kontrolą nośników danych USB
5	Wprowadzenie do systemu	Omówienie funkcjonalności systemu, jego architektury oraz podstawowych mechanizmów działania. Przedstawienie najlepszych praktyk zarządzania oprogramowaniem.
6	Konsultacje	Wykonawca zapewni możliwość konsultacji technicznych w okresie 30 dni po zakończeniu szkolenia w celu wyjaśnienia ewentualnych problemów.
7	Materiały szkoleniowe	Wykonawca dostarczy materiały szkoleniowe w formie elektronicznej, zawierające instrukcje, przykłady konfiguracji oraz procedury administracyjne.
8	Egzamin końcowy i certyfikacja	Po zakończeniu szkolenia uczestnik podejdzie do testu wiedzy, a w przypadku pozytywnego wyniku otrzyma certyfikat potwierdzający ukończenie szkolenia. Wynik testu ma charakter wyłącznie informacyjny i nie wpływa na ocenę wykonania przedmiotu zamówienia.

3.13 Zadanie 13: Zakup szkolenia dla pracowników wydziału informatyki z technologii Windows Server

L.p.	Wymaganie	Opis wymagania
1	Przedmiot zamówienia	Przedmiotem zamówienia jest zakup szkolenia dla 1 pracownika z technologii Windows Server. Szkolenie musi być prowadzone przez osobę posiadającą udokumentowaną wiedzę i doświadczenie w zakresie administracji systemami Windows Server oraz realizacji szkoleń z tego zakresu. Zamawiający preferuje, aby osoba prowadząca posiadała status trenera certyfikowanego przez Microsoft, lecz nie jest to warunek obligatoryjny.
2	Liczba uczestników	Szkolenie przeznaczone jest dla jednego pracownika Urzędu Gminy w Białym Borze.

3	Wymagania dotyczące szkoleń	Zamawiający dopuszcza szkolenia równoważne pod względem zakresu tematycznego i efektów kształcenia, prowadzone na podstawie programu zgodnego z zakresem technologii Windows Server.
4	Administracja Windows Server	Szkolenie obejmuje wprowadzenie do systemu Windows Server, Windows Server Core oraz narzędzi administracyjnych.
5	Zarządzanie tożsamością	Szkolenie obejmuje zarządzanie Active Directory Domain Services (AD DS), wdrażanie kontrolerów domeny, polityki grupowe (GPO) oraz usługi certyfikatów AD.
6	Zarządzanie infrastrukturą sieciową	Obejmuje konfigurację i zarządzanie DHCP, DNS, IPAM oraz usługami dostępu zdalnego.
7	Zarządzanie serwerami plików	Szkolenie obejmuje konfigurację serwerów plików, deduplikację danych oraz obsługę iSCSI.
8	Wirtualizacja Hyper-V i zarządzanie kontenerami	Wdrażanie, konfiguracja i zabezpieczenie maszyn wirtualnych oraz kontenerów w środowisku Windows Server.
9	Konfiguracja JEA i analiza ruchu SMB	Szkolenie obejmuje Just Enough Administration (JEA), analizę ruchu SMB oraz zarządzanie aktualizacjami systemu.
10	Monitorowanie wydajności i rozwiązywanie problemów	Szkolenie obejmuje narzędzia do monitorowania i diagnozowania wydajności systemu Windows Server.
11	Wdrażanie usług pulpitu zdalnego (RDS) i usług zdalnego dostępu	Konfiguracja i zarządzanie VPN, Always On VPN oraz Network Policy Server (NPS).
12	Aktualizacje i migracje	Migracja Active Directory Domain Services (AD DS) oraz usługi migracji pamięci masowej w środowisku Windows Server.
13	Forma szkolenia	Szkolenie musi być prowadzone w formie praktycznych warsztatów z wykorzystaniem środowiska testowego. Szkolenie musi odbywać się w języku polskim. Zamawiający dopuszcza formę szkolenia online - na żywo.
14	Liczba godzin szkolenia	Szkolenie musi obejmować co najmniej 30 godzin zajęć.
15	Certyfikacja	Po zakończeniu szkolenia uczestnik

		powinien otrzymać certyfikat potwierdzający udział w szkoleniu i nabycie wiedzy zgodnej z zakresem programowym.
--	--	---