**Załącznik nr 6 do SWZ**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zamówienie podzielone jest na części:**

* **Część 1 – Dostawa, wstępna konfiguracja oraz uruchomienie serwerów wraz z wymaganymi licencjami, konfiguracja usługi katalogowej wraz z migracją profili lokalnych oraz wirtualizacja posiadanej infrastruktury serwerowej i wdrożenie usługi dystrybucji aktualizacji wraz z dostawą szafy RACK**
* **Część 2 – konfiguracja systemu kopii zapasowej**
* **Część 3 – Dostawa, wstępna konfiguracja oraz uruchomienie macierzy dyskowej wraz z dostawą szafy RACK oraz systemem podtrzymania bateryjnego dla macierzy dyskowej**
* **Część 4 - usługa wsparcia środowiska IT Zamawiającego**
* **Część 5 – Zapewnienie systemu monitoringu stanu infrastruktury IT Zamawiającego**
* **Część 6 - Szkolenia z zakresu rozwiązań technicznych**
* **Część 7 - Dostarczenie i wdrożenie urządzenia UTM klasy NGF**
* **Część 8 - Modernizacja infrastruktury sieciowej**
* **Część 9 - Szkolenia z zakresu cyberbezpieczeństwa**
* **Część 10 - Dostarczenie stacji roboczych**
* **Część 11 - Wykonania usługi polegającej na zaprojektowaniu, utworzeniu i świadczeniu usługi chmurowej w postaci serwisu www dla Gminy Sępólno Krajeńskie**

**Część 1**

**Dostawa, wstępna konfiguracja oraz uruchomienie serwerów wraz z wymaganymi licencjami, konfiguracja usługi katalogowej wraz z migracją profili lokalnych oraz wirtualizacja posiadanej infrastruktury serwerowej i wdrożenie usługi dystrybucji aktualizacji wraz z dostawą szafy RACK**

* 1. **Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach;
2. konfiguracja, instalacja serwerów oraz wirtualizacja wskazanych zasobów Zamawiającego wraz z uruchomieniem środowiska;
3. konfiguracja usługi katalogowej;
4. migracja profili lokalnych stacji roboczych używanych przez pracowników Zamawiającego do usługi katalogowej w kooperacji z Działem IT Zamawiającego;
5. utworzenie polityki bezpieczeństwa w dziedzinie haseł;
6. konfiguracja polityk w oparciu o wskazania Zamawiającego (4 polityki);
7. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;
8. wdrożenie rozwiązania automatycznej dystrybucji aktualizacji systemowych dla środowiska opartego o systemy klienckie oprogramowania systemowego stosowanego już istniejącego w infrastrukturze Urzędu Miejskiego w Sępólnie Krajeńskim.
9. dostawa Oprogramowania i zapewnienie możliwości korzystania przez Zamawiającego z Oprogramowania na warunkach licencyjnych mających zastosowanie do Oprogramowania;
10. dostarczenie szafy RACK 19” 42U.

**1.2 Termin realizacji zamówienia oraz liczba dostarczanego sprzętu**

Zamawiający wymaga, aby dostawa sprzętu wraz z instalacją i wdrożeniem u Zamawiającego, o którym mowa w pkt 1.1 nastąpiła w terminie 21 dni od dnia zawarcia umowy.

**1.3 Wymagania szczegółowe Zamawiającego**

**Zestawienie wymaganych parametrów technicznych serwera (2 sztuki)**

|  |  |
| --- | --- |
| **Nazwa elementu lub cechy** | **Parametry**  |
| **Obudowa** | Do instalacji w szafie Rack 19", wysokość nie mniej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych; |
| **Procesor** | * Zainstalowane 2 procesory w architekturze x64, Ilość rdzeni / wątków min. 16 / min. 32.
 |
| **Płyta główna** | * Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera;
* Wyposażona w moduł TPM 2.0;
* Minimum 32 sloty DIMM na pamięć DDR4;
 |
| **Pamięć operacyjna** | * Zainstalowane minimum 128GB pamięci RAM o częstotliwości minimum 3200MHz;
* Możliwość rozbudowy/rekonfiguarcji serwera do 8TB pamięci RAM DDR4;
 |
| **Zabezpieczenie pamięci** | Wsparcie dla: memory mirroring, ECC, SDDC lub Advanced ECC; |
| **Procesor Graficzny** | * Zintegrowana karta graficzna z minimum 16MB pamięci, osiągająca rozdzielczość 1920x1200 przy 60 Hz;
* 1 port VGA na tylnym panelu serwera oraz jeden port VGA na panelu przednim;
* Możliwość instalacji dodatkowej karty GPU posiadającą 4 porty mDP lub DP lub HDMI;
 |
| **Zatoki dyskowe i dyski** | * Serwer wyposażony w min. 8 zatok dyskowych hot-plug 2.5” umożliwiających instalację dysków SSD/HDD interfejsem SAS/SATA;
* Serwer wyposażony w min. 4 dyski SATA SSD o pojemności min. 960GB każdy. Dyski klasy Enterprise dedykowane do pracy w oferowanym serwerze i o parametrze DWPD min. 1;
* Możliwość rozbudowy serwera o 2 dyski M.2 SSD NVMe o pojemności min. 960GB. Rozwiązanie dedykowane jako nośnik boot, musi umożliwiać konfigurację sprzętowego mirroringu (RAID 1).
 |
| **Kontroler dyskowy** | * Serwer wyposażony w sprzętowy kontroler RAID obsługujący dyski SAS 3.0 i pozwalający na konfigurację RAID 0,1,10,5;
* Serwer umożliwiający rozbudowę/rekonfigurację o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 2 GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler obsługujący funkcjonalność SSD Cache na poziomie sprzętowym tj. możliwość wykorzystania dysku SSD do przyśpieszenia operacji odczytu dla grupy RAID na dyskach HDD.
 |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy min. 800W z certyfikatem minimum Platinum. |
| **Interfejsy sieciowe** | * min. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
* Karta LAN posiadająca min. 2 porty 10GbE BASE-T oraz min. dwa porty 1GbE BASE-T nie zajmujące slotów PCIe serwera;
 |
| **Sloty PCIe** | * Serwer posiadający – w momencie dostarczenia – min. 2 sloty PCIe generacji 4.0 w tym 1 slot działający z prędkością x16;
* W momencie dostarczenia min. jeden slot PCIe powinien być wolny, dostępny dla użytkownika;
 |
| **Dodatkowe porty** | * z przodu obudowy: min. 1x USB 3.0, min. 1x VGA
* z tyłu obudowy: min. 2x USB 3.0, min. 1x VGA
* wewnętrzne: min. 1 x USB 3.0
 |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |
| **Zarządzanie** | Serwer musi posiadać moduł zarządzający wyposażony w minimum jeden port 10/100/1000 Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł musi umożliwiać:* monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe
* dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub
* dostęp do karty możliwy:
	+ z poziomu przeglądarki webowej (GUI)
	+ z poziomu linii komend (SSH lub IPMI)
* wbudowane narzędzia diagnostyczne
* zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego
* obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
* wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
* przesyłanie alertów poprzez e-mail oraz SNMP
* obsługa zdalnego serwera logowania (remote syslog)
* wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB
* funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy)
* monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
* konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
* zdalna aktualizacja oprogramowania (firmware)
* możliwość równoczesnej obsługi przez min. 2 administratorów
* wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
 |
| **Funkcje zabezpieczeń** | * Czujnik otwarcia obudowy;
* Ramka zabezpieczająca przed nieautoryzowanym dostępem do dysków serwera;
 |
| **Urządzenia hot swap** | Dyski twarde, zasilacze, wentylatory. |
| **Wspierane systemy operacyjne** | Microsoft Windows Server 2019, 2022, Red Hat Enterprise Linux 8, VMware vSphere (ESXi) 7.0;  |
| **Gwarancja** | * min. 36 miesięcy wsparcia producenta w trybie pełnego serwisu on-site NBD. Przy czym NBD określa czas reakcji w miejscu instalacji sprzętu;
* W przypadku awarii dyski twarde pozostają własnością zamawiającego;
* Usługa wsparcia technicznego musi być świadczona przez producenta lub autoryzowany serwis producenta oferowanych urządzeń;
 |
| **Inne** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001;
* Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA;
* Możliwość rozbudowy serwerów zgodnie z ww. opisem przedmiotu zamówienia musi być możliwa przy użyciu certyfikowanych komponentów oraz zachowaniu pełnego wsparcia i gwarancji producenta serwera;
* Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce;
 |
| **Licencje** | * Dostarczenie 55 sztuk Licencji na Server do stacji roboczych zainstalowanych w urzędzie. Licencje muszą być nie przypisane do sprzętu.
 |

Punktacja dodatkowa:

|  |  |
| --- | --- |
| **Parametr dodatkowy 1** | Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanych serwerów, nawet po wygaśnięciu okresu wsparcia.  |
| **Parametr dodatkowy 2** | Oprogramowanie diagnostyczne producenta serwera (lub wbudowana funkcja karty zarządzającej) posiadające funkcjonalność predykcji awarii wszystkich kluczowych komponentów serwera: procesorów, pamięci RAM, dysków wewnętrznych HDD/SSD/M.2 SSD, wentylatorów, zasilaczy, kontrolerów dyskowych.  |
| **Parametr dodatkowy 3** | Serwer wyposażony w wbudowany panel LCD umieszczony na froncie obudowy i pozwalający na wyświetlenie informacji o: stanie serwera, konfiguracji sieciowej karty zarządzającej, zasilaniu, temperaturze. |
| **Parametr dodatkowy 4** | Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS. |

**Zestawienie wymaganych parametrów technicznych szafy RACK**

1. Szafa rack o wysokości 42U 19”
2. Szafa stojąca,
3. Otwory wentylacyjne w dolnej i górnej płycie szafy oraz w drzwiach
4. Drzwi przednie perforowane metalowe (siatka),
5. Drzwi tylne pełne lub perforowane,
6. Maksymalne wymiary zewnętrzne 800x800x2047.5 mm
7. Kolor: czarny
8. Maksymalne obciążenie statyczne do 800 kg
9. Szafa do złożenia na miejscu przez Wykonawcę we wskazanym pomieszczeniu

 **1.4 Zestawienie wymaganych parametrów technicznych odnośnie systemów operacyjnych:**

1. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.
2. Wbudowane wsparcie instalacji i pracy na wolumenach które:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,
	4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
3. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
4. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
5. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
6. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
7. Wbudowana zapora internetowa (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
8. Graficzny interfejs użytkownika.
9. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
10. Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.
11. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
12. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
13. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarzadzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
		1. podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		2. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		3. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
14. Zdalna dystrybucja oprogramowania na stacje robocze.
15. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
16. PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
	1. dystrybucję certyfikatów poprzez http,
	2. konsolidację CA dla wielu lasów domeny,
	3. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
17. Szyfrowanie plików i folderów.
18. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
19. Serwis udostępniania stron WWW
20. Wsparcie dla protokołu IP w wersji 6 (Ipv6).
21. Wbudowane usługi VPN pozwalające na zestawienie równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem zainstalowanymi obecnie w urzędzie.

**1.5 Wymagane prace wdrożeniowe**

1. **Dostarczenie sprzętu wraz z konfiguracją i wirtualizacją zasobów**
	1. Zinwentaryzowanie i walidacja aktualnego środowiska serwerowego objętego migracją
	2. Dedykowane wsparcie aplikacji dziedzinowych realizuje migrację aplikacji do nowego środowiska na wniosek Zamawiającego.
	3. Podłączenie serwerów do infrastruktury elektrycznej i sieciowej Zamawiającego
	4. Wstępna konfiguracja serwerów polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowego do najnowszej zalecanej przez producenta wersji
	5. Przygotowanie środowiska wirtualizacji na nowo dostarczonych serwerach
	6. Przygotowanie 4 maszyn wirtualnych opartych na najnowszym systemie serwerowym, dostępnej wersji
	7. Przekazanie dostępów Zamawiającemu
	8. Testy po uruchomieniu środowiska wirtualnego polegające na sprawdzeniu poprawności uruchamiania się środowiska systemowego i poprawności pracy systemu replikacji
	9. Uruchomienie replikacji dla wskazanych min 4 maszyn wirtualnych
	10. Drugi dostarczony serwer pełnić ma rolę repozytorium replik i ma służyć awaryjnemu uruchomieniu środowiska
	11. Przygotowanie dokumentacji powdrożeniowej zawierającej opis wdrożonej konfiguracji wirtualizacji zasobów
2. **Wymagania odnośnie środowiska wirtualizacji:**
	1. Możliwość obsługi Secure Boot oraz Trusted Platform Module
	2. Możliwość rozruchu PXE z syntetyczną kartą sieciową
	3. Możliwość rozruchu z dysku SCSI
	4. Możliwość obsługi dysków wirtualnych w formacie .vhdx
	5. Wsparcie dla UEFI z GPT
	6. Obsługa 32-bitowych i 64-bitowych systemów operacyjnych
	7. Obsługa do 12TB pamięci RAM
	8. Obsługa do 240 procesorów wirtualnych
	9. Wsparcie dla Intel VT oraz AMD-V
	10. Obsługa replikacji między hostami oraz klastrów wysokiej dostępności (failover cluster)
	11. Wirtualizator musi pozwalać na zmianę parametrów maszyny wirtualnej
	12. Wirtualizator musi zapewniać możliwość zatrzymywania, uruchamiania i restartowania maszyn wirtualnych
	13. Wirtualizator musi umożliwiać tworzenie wirtualnych przełączników
	14. Wirtualizator musi zapewniać wbudowane mechanizmy do migracji na żywo maszyn wirtualnych, migracji magazynu oraz funkcję importu/eksportu maszyny wirtualnej
	15. Wirtualizator musi zapewniać możliwość tworzenia kopii maszyn wirtualnych w innych lokalizacjach fizycznych (mechanizmy replikacji), kopiowania woluminów w tle oraz budowanie klastrów wysokiej dostępności
3. **Wdrożenie usługi katalogowej w infrastrukturze Zamawiającego**
	1. Wykonawca zobowiązuje się do dostarczenia 55 licencji USER CAL potrzebnych do wdrożenia usługi katalogowej
	2. Utworzenie maszyny wirtualnej na hypervisorze pełniącej rolę kontrolera domeny
	3. Utworzenie domeny usługi katalogowej
	4. Utworzenie schematu organizacyjnego oraz nadanie odpowiednich uprawnień poszczególnym użytkownikom, po ustaleniach z Zamawiającym
	5. Konfiguracja polityki bezpieczeństwa haseł
	6. Utworzenie 4 polityk w oparciu o wskazania zamawiającego
	7. Podłączenie komputerów do utworzonej domeny – proces wykonywany wspólnie z administratorem IT Zamawiającego, na bazie ustalonego harmonogramu
	8. Migracja profili lokalnych ze stacji roboczych użytkowników do usługi katalogowej – proces wykonywany wspólnie z administratorem IT Zamawiającego, na bazie ustalonego harmonogramu
	9. Instalacja odpowiednich, wskazanych przez Zamawiającego drukarek na poszczególnych stacjach roboczych wraz z działem IT Zamawiającego
	10. Dokumentowanie wykonanych prac
4. **Wdrożenie systemu automatycznej dystrybucji aktualizacji systemów operacyjnych w infrastrukturze IT Zamawiającego**
	1. System musi działać w ramach posiadanych i dostarczonych licencji
	2. System musi zapewniać możliwość identyfikacji aktualizacji do zainstalowania na stacjach roboczych,
	3. system musi zapewnić możliwość pobierania aktualizacji na wskazane lokalne repozytorium po godzinach pracy Urzędu
	4. Dystrybucja aktualizacji musi wykonywać się w ramach infrastruktury lokalnej LAN w czasie pracy, po godzinach pracy Urzędu
	5. System musi zapewnić możliwość wycofywania aktualizacji w przypadku zidentyfikowania nieprawidłowości funkcjonalnych

**Część 2**

**Konfiguracja systemu kopii zapasowej**

**2.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. dostawa systemu kopii zapasowych;
2. wdrożenie oraz konfiguracja systemu kopii zapasowych w środowisku IT Zamawiającego
3. dostarczenie przez Wykonawcę dokumentacji konfiguracji wdrożonego systemu

**2.2 Termin realizacji zamówienia oraz liczba dostarczanego sprzętu**

Zamawiający wymaga, aby dostawa systemu wraz z wdrożeniem i konfiguracją, o którym mowa w pkt 2.1 do Zamawiającego nastąpiła w terminie 5dni od dnia zrealizowania części 1.

Zamawiający poinformuje Wykonawcę przez ePUAP o zrealizowaniu części 1.

**2.3 Wymagania szczegółowe Zamawiającego:**

|  |
| --- |
| 1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
 |
| 1. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
 |
| 1. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
 |
| 1. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych na zasobach obecnych w Urzędzie Miejskim w Sępólnie Krajeńskim.
 |
| 1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
 |
| 1. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
 |
| 1. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental)
 |
| 1. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
 |
| 1. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
 |
| 1. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy aktualizowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.
 |
| 1. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania migawki.
 |
| 1. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
 |
| 1. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej opisie przedmiotu zamówienia.
 |
| 1. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).
 |
| 1. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
 |
| 1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
 |
| 1. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
 |
| 1. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
 |
| 1. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
 |
| 1. Oprogramowanie musi wspierać BlockClone API w przypadku użycia serwera o najnowszej aktualizacji z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
 |
| 1. Repozytoria oparte o XFS muszą pozwalać na zmienność danych przez określoną ilość czasu (tzw. Immutability)
 |
| 1. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
 |
| 1. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
 |
| 1. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
 |
| 1. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
 |
| 1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
 |
| 1. Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
 |
| 1. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
 |
| 1. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.
 |
| 1. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
 |
| 1. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
 |
| 1. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
 |
| 1. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
 |
| 1. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików wykorzystywanych w Urzędzie Miejskim w Sępólnie Krajeńskim z następujących systemów plików:
 |
| 1. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
 |
| 1. Oprogramowanie musi wspierać granularne odtwarzanie obiektów usługi katalogowej takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
 |
| 1. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
 |
| 1. Oprogramowanie musi wspierać granularne odtwarzanie SQL w starszych i nowych wersjach, również wykorzystywanych w urzędzie.
 |
| 1. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
 |
| 1. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD - oprogramowanie wykorzystywane w Urzędzie Miejskim w Sępólnie Krajeńskim.
2. Oprogramowanie musi zapewniać możliwość wykonywania kopii zapasowych minimum 8 maszyn wirtualnych oraz min. 2 hostów fizycznych.
3. Oprogramowanie musi zapewniać możliwość wykonywania kopii zapasowych minimum 55 stacji roboczych.
 |

**2.4 Wymagane prace wdrożeniowe**

1. instalacja oprogramowania do kopii zapasowych na zasobie wirtualnym wskazanym przez Zamawiającego;
2. skonfigurowanie repozytorium kopii zapasowych wskazanego przez Zamawiającego
3. zaprojektowanie i wdrożenie polityki tworzenia kopii zapasowych z wykorzystaniem dostarczonego oprogramowania do kopii zapasowych dla przynajmniej 8 maszyn wirtualnych, 2 hostów fizycznych oraz 55 stacji roboczych;
4. przeprowadzenie testów akceptacyjnych poprawności działania operacji, kopii zapasowych i odzyskiwania danych;
5. konfiguracja powiadomień systemu kopii zapasowej oraz weryfikacja ich działania;
6. szkolenie z systemu kopii zapasowych obejmujące:
	1. przybliżenie interfejsu rozwiązania i funkcjonalności
	2. tworzenie zadań kopii zapasowych
	3. tworzenie powiadomień, walidacji wykonywania się kopii zapasowych

dobrych praktyk w dziedzinie administracji i obsługi systemów kopii zapasowych.

**Część 3**

**Dostawa, wstępna konfiguracja oraz uruchomienie macierzy dyskowej wraz z dostawą szafy RACK oraz systemem podtrzymania bateryjnego dla macierzy dyskowej**

**3.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach;
2. konfiguracja urządzenia oraz fizyczna instalacja w infrastrukturze IT Zamawiającego;
3. udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
4. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;

**3.2 Termin realizacji zamówienia**

Zamawiający wymaga, aby dostawa sprzętu wraz z konfiguracją, o których mowa w pkt 3.1 do Zamawiającego nastąpiła w terminie 7 dni od dnia zawarcia Umowy.

**3.3 Wymagania szczegółowe Zamawiającego**

**Zestawienie wymaganych parametrów technicznych macierzy dyskowej**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Wymagania ogólne | Do instalacji w standardowej szafie RACK 19 wraz z kompletem szyn do montażu w szafie Rack. Całość rozwiązania nie może zajmować więcej niż 1U w szafie RACK. Wraz z urządzeniem muszą być dostarczone elementy montażowe umożliwiające instalację we wszystkich zatokach dysków twardych zarówno 3,5” jak i 2,5” (kieszenie, śrubki montażowe) |
| RAID | Wymagana obsługa: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, RAID 60, JBOD, Single |
| Szyfrowanie danych | Z wykorzystaniem AES-256bit |
| Pamięć RAM | Zainstalowane minimum 4GB DDR4 UDIMM (1x2GB) |
| Pamięć flash | Zainstalowane minimum 512MB (ochrona systemu operacyjnego przed podwójnym rozruchem) |
| Porty Ethernet | 2 x 10GbE SFP+2 x 2.5 Gigabit Ethernet Port |
| Porty USB | 4 porty USB 3.2 Gen 1 |
| Sloty PCI | Minimum 1x PCIe Gen 2 x2, przy czym minimum 1 slot wolny, udostępnione pod dalszą rozbudowę po obsadzeniu wymaganymi kartami.  |
| Wymagania ogólne | 4 wewnętrzne kieszenie na dyski, w których można zastosować dyski 2,5” oraz 3,5”, HDD oraz SSD z interfejsem SATA 6Gb/s |
| Cache SSD | Urządzenie musi wspierać technologię SSD Cache pozwalającą rozbudować pamięć podręczną odczytu z wykorzystaniem nośników SSD |
| Dyski HDD | 4 sztuki dysków HDD SATA 3,5” o prędkości obrotowej minimum 7200 obr/min i pojemności minimum 4TB każdy. Kompatybilne z proponowanym rozwiązaniem NAS. |
| Obsługiwane formaty zewnętrznych dysków twardych | EXT3, EXT4, NTFS, FAT32, HFS+ |
| Interfejs systemu operacyjnego | Graficzny, pozwalający na wielowątkową równoległą pracę uruchomionych procesów/aplikacji, minimum w językach angielskim i polskim |
| Wymagania ogólne | Wsparcie dla protokołów:SSH, Telnet, HTTP(S), FTP, CIFS/SMB, AFP, iSCSI, FibreChannel, NFS, SNMP, VPN |
| Natywny system plików | Urządzenie musi natywnie pracować w oparciu o system plików obsługujący pojedynczy wolumin o pojemności do min. 250 TBMożliwość utworzenia minimum 128 wolumenów |
| Wymagania ogólne | Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju. Wymagane jest dostarczenie oświadczenia potwierdzającego wydane przez producenta.  |
| Zasilanie | Minimum 250 W PSU, 100-240V |
| Waga | Netto – maksymalnie 6,6kgBrutto – maksymalnie 9,6kg |
| Maksymalny pobór mocy | 40 W |
| Gwarancja producenta sprzętu | Minimum 36 miesięcy gwarancji producenta. Jeżeli w standardzie urządzenie ma inny okres należy w ofercie podać nazwę i typ pakietu rozszerzającego gwarancję producenta. Gwarancja realizowana w trybie następny dzień roboczy – udostępniający urządzenie zastępcze na czas naprawy. Wymiana dysków może być dokonywana przez Zamawiającego |

**Zestawienie wymaganych parametrów technicznych szafy RACK**

1. Szafa rack o wysokości 12U 19”
2. Szafa do zawieszenia na ścianie
3. Otwory wentylacyjne w dolnej i górnej płycie szafy oraz w drzwiach
4. Drzwi przednie z przeszkleniem, zamykane zamkiem na klucz
5. Maksymalne wymiary zewnętrzne 570x635x450 mm
6. Kolor: czarny
7. Maksymalne obciążenie statyczne do 60 kg
8. Szafa do złożenia na miejscu przez Wykonawcę we wskazanym pomieszczeniu

**Zestawienie wymaganych parametrów technicznych systemu podtrzymania bateryjnego**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Moc znamionowa w W | minimum 410 W |
| Moc znamionowa w VA | minimum 750 VA |
| Rodzaj akumulatora | kwasowo-ołowiowy |
| czas pełnego ładowania | max. 8 godzin |
| Pojemność baterii | minimum 7 Ah |
| Żywotność baterii | minimum 3 lata |
| Ochrona linii danych | Ochrona kabli sieci Ethernet RJ45 10/100/1000 Base-T |
| Masa produktu | Maksymalnie 5,2 kg |
| Sposób montażu | wolnostojący |
| Komunikacja i zarządzanie | * Dioda led wskazująca status zasilania
* Alarm niskiego poziomu naładowania akumulatora
 |
| Certyfikaty produktu | CE, CB, EAC |
| Normy produktu | EN/IEC 62040-1EN/IEC 62040-2CE |
| Gwarancja | minimum 36 miesięcy |

**3.4 Wymagane prace wdrożeniowe**

1. dostarczenie fabrycznie nowego sprzętu;
2. instalacja sprzętu w dostarczonej szafie rack;
3. podłączenie sprzętu do instalacji elektrycznej;
4. podłączenie sprzętu do infrastruktury sieciowej Zamawiającego we wskazane porty;
5. wstępna konfiguracja urządzenia polegająca na aktualizacji firmware’u do możliwie jak najwyższej i stabilnej wersji oprogramowania (zalecanej przez producenta urządzenia);
6. utworzenie kont dostępowych dla dostępu administracyjnego do urządzenia;
7. zweryfikowanie poprawności działania systemu podtrzymania bateryjnego;
8. ustanowienie urządzenia jako repozytorium kopii zapasowych maszyn wskazanych przez Zamawiającego

**Część 4**

**Usługa wsparcia środowiska IT Zamawiającego**

**4.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. Świadczenie kompleksowej usługi wsparcia w zakresie merytoryczno konsultacyjnym w dziedzinie infrastruktury IT Zamawiającego

**4.2 Termin realizacji zamówienia**

Zamawiający wymaga, aby świadczenie kompleksowej usługi wsparcia, o której mowa w pkt 4.1 trwała w terminie 7 miesięcy od dnia zawarcia umowy.

**4.3 Szczegółowe wymagania odnośnie usługi**

1. Usługa wsparcia ma być realizowana w następujących obszarach:
	1. Wsparcie utrzymaniowe infrastruktury IT – pomoc w analizie i rozwiązywaniu problemów infrastrukturalnych (urządzenie brzegowe, urządzenia sieciowe typu przełącznik, serwery fizyczne, serwery z wirtualizacją, NAS, konfigurowanie usług serwera)
	2. Wsparcie konsultacyjne – umożliwienie realizacji konsultacji odnośnie ścieżek rozwoju i zmian w infrastrukturze Zamawiającego, propozycje zmian konfiguracyjnych, zakupowych i aktualizacyjnych wedle potrzeb
	3. Dostęp do 5 webinariów dotyczących problematyki administracyjnej i bezpieczeństwa zasobów IT
2. Rozpoczęcie współpracy i wdrożenie usługi wsparcia musi wiązać się z inwentaryzacją zasobów IT Zamawiającego przez Wykonawcę, dopuszcza się realizację procesu inwentaryzacji zdalnie lub w siedzibie Zamawiającego wraz z osobą odpowiedzialną za obszar IT po stronie Zamawiającego
3. Wsparcie ma być realizowane w zakresie 54 godzin przypadających na okres 7 miesięcy trwania umowy, to jest 8 godzin przez 5 miesięcy, ostatnie 2 miesiące po 7 godzin.
4. Niewykorzystane godziny w 1 miesięcznym okresie rozliczeniowym nie przechodzą do następnego okresu rozliczeniowego
5. Zamawiający akceptuje formę zdalną poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego
6. W ramach pakietu miesięcznej liczby godzin wsparcia realizowane są działania dotyczą diagnostyki i naprawy problemów występujących w infrastrukturze Zamawiającego oraz spotkania konsultacyjne
7. Kontakt w ramach usługi wsparcia musi być realizowany za pośrednictwem infolinii, komunikacji e-mail lub systemu formularzy, przy czym Zamawiający wymaga utrzymania minimum 2 form kontaktu z wcześniej wymienionych
8. Wsparcie musi być realizowane w oparciu o SLA jak w tabeli poniżej:

|  |  |  |
| --- | --- | --- |
| **Priorytet** | **Czas realizacji (rh)** | **Czas reakcji (rh)** |
| **Krytyczny** | 4 | 1 |
| **Wysoki** | 6 | 1 |
| **Średni** | 10 | 1 |
| **Niski** | 24 | 1 |
| **Wniosek** | 40 | 1 |
| **Zdarzenie** | -- | 1 |

\* rh – roboczogodzina

Natomiast sam status nadawania priorytetów zgłaszanym zadaniom ma odbywać się w oparciu o niniejszą tabelę priorytetów:

|  |  |
| --- | --- |
|  | Pilność |
| WPŁYW | **Praca uniemożliwiona** | **Utrudnienie pracy****(istnieje alternatywa)** | **Prace Planowe** | **Wniosek o usługę** | **Zdarzenie** |
| **Cała organizacja** | Krytyczny | Krytyczny | Średni | Wniosek | Zdarzenie |
| **Kilka Lokacji** | Krytyczny | Wysoki | Średni | Wniosek | Zdarzenie |
| **Grupa użytkowników** | Wysoki | Wysoki | Niski | Wniosek | Zdarzenie |
| **Pojedynczy użytkownik** | Średni | Niski | Niski | Wniosek | Zdarzenie |

Gdzie zamawiający definiuje pojęcia jak niżej:

Wpływ – jest jednostką mierzalności krytyczności dla biznesu, dotyczącą incydentów lub problemów.
Wpływ jest mierzony liczbą ludzi lub systemów zaangażowanych.

|  |  |
| --- | --- |
| **Wpływ** | **Opis** |
| **1. Cała organizacja** | Wszyscy autoryzowani użytkownicy. |
| **2. Kilka lokacji**  | Wszyscy autoryzowani użytkownicy z kilku lokacji. |
| **3. Niewielka grupa użytkowników**  | Wszyscy autoryzowani użytkownicy z jednej lokacji / zespołu. |
| **4. Pojedynczy użytkownik**  | Indywidualne zgłoszenie. |

Pilność – jest określeniem szybkości rozwiązywania incydentów posiadających konkretny wpływ.

|  |  |
| --- | --- |
| **Pilność** | **Opis** |
| **1. Praca uniemożliwiona** | Poważny defekt prowadzący do całkowitego przerwania procesów biznesowych po stronie klienta. Nie istnieje obejście problemu / doraźne rozwiązanie. Wykonywanie pracy jest niemożliwe. |
| **2. Utrudnienie pracy (istnieje obejście)** | Defekt mający wpływ na procesy biznesowe po stronie klienta, przerwany przepływ operacyjny. Dysfunkcja podstawowych narzędzi lub aplikacji. Praca jest utrudniona, ale możliwa. |
| **3. Niska pilność / planowane** | Utrudnienie mające wpływ na pracę użytkownika, lecz jego pilność jest niewysoka i rozwiązanie może być zaplanowane w czasie. |
| **4. Wniosek o usługę / pytanie** | Dotyczy wniosku o usługę lub zapytania, a nie incydentu. |

1. Dostęp do wsparcia musi być realizowany w systemie 24/7/365, zgłoszenia w charakterze incydentów, wniosków i zdarzeń muszą być podejmowane i realizowane od poniedziałku do piątku w godzinach 7:00 – 17:00, natomiast w godzinach 17:00 – 7:00 oraz w dni wolne od pracy i weekendy, podmiot świadczący musi zapewnić inżyniera dyżurnego, który jest w stanie podjąć działania na wypadek zdarzeń krytycznych, które wystąpią w czasie poza godzinami pracy zamawiającego lub na wypadek incydentów zgłoszonych w tych porach przez administratora zasobów IT Zamawiającego

**Część 5**

**Zapewnienie systemu monitoringu stanu infrastruktury IT Zamawiającego**

**5.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. Dostawa, instalacja systemu monitoringu dla infrastruktury IT Zamawiającego;
2. przeprowadzenie szkolenia z posługiwania się dostarczonym rozwiązaniem i interpretacji danych prezentowanych przez system monitoringu.

**5.2 Termin realizacji zamówienia**Zamawiający wymaga, aby dostawa, instalacja oprogramowania, o którym mowa w pkt 5.1 do Zamawiającego nastąpiła w terminie 7 dni od dnia zawarcia Umowy.

**5.2 Szczegółowe wymagania odnośnie proponowanego rozwiązania**

1. System powinien być uruchomiony na zasobach infrastruktury IT Zamawiającego.
2. System powinien być zrealizowany na środowisku nie wymagającym licencjonowania systemu operacyjnego maszyny wirtualnej
3. System powinien agregować dane o statusie maszyn wirtualnych realizowanych na wirtualizatorze Microsoft HYPER-V oraz VMWare
4. W przypadku systemów z rodziny Microsoft Windows Server oraz Linux, system powinien zapewniać możliwość zdefiniowania kluczowych usług, których wyłączenie lub przerwa w działaniu będzie monitowana - serwisów uruchomionych na powłoce Windows/Linux, statusu baz danych MSSQL Express i Standard, PostgresSQL, Firebird
5. System musi zapewniać możliwość odczytu danych z urządzeń przy wykorzystaniu protokołu SNMP, IMPI, JMX
6. System musi zapewniać możliwość ostrzegania w przypadku braku odpowiedzi z monitorowanego urządzenia, maszyny wirtualnej, serwera fizycznego
7. System powinien integrować się z rozwiązaniami do zdalnego zarządzania serwerami takimi jak: iDRAC, iLO, XClarity Controller
8. System powinien pozwalać. na uzyskiwanie informacji o utylizacji CPU, RAM, przestrzeni pamięci masowej, interfejsów sieciowych maszyn wirtualnych opartych o Linux, Windows
9. System powinien zapewniać możliwość odczytu stanu CPU, wentylatorów, temperatury, utylizacji interfejsów urządzeń sieciowych wiodących producentów jak Ubiquiti, DELL, Extreme, Fortinet, CISCO i innych zapewniających komunikację SNMP z urządzeniem
10. System powinien umożliwiać dla monitorowanych elementów natychmiastowe graficzne przedstawienie na wykresie za pomocą wbudowanej funkcjonalności
11. System graficznego przedstawienia (wykresy) powinien posiadać funkcje:
	1. możliwości tworzenia niestandardowych wykresów;
	2. łączenia wielu elementów w jeden widok
	3. tworzenia mapy sieci
	4. tworzenia raportów
12. System powinien mieć funkcjonalność pozwalającą na tworzenie szablonów konfiguracji serwerów
13. System powinien zapewniać możliwość wykonania automatycznego wykrywania urządzeń sieciowych w danym obszarze
14. System powinien zapewniać możliwość automatycznej rejestracji agenta
15. System powinien zapewniać programowalny interfejs API
16. System musi zapewniać możliwość definiowania czasu retencji przechowywania danych oraz progów ostrzeżeń:
	1. Warning – rozumianych jako ostrzeżenie
	2. Critical – rozumianych jako rzutujących na całą infrastrukturę Zamawiającego i uniemożliwiające wykonywanie czynność)
17. System powinien zapewniać możliwość wysyłki monitów w postaci e-mail oraz opcjonalnie powinien zapewniać możliwość integracji z rozwiązaniami typu bramka sms
18. System powinien zapewniać możliwość bezpiecznego uwierzytelniania oraz nadawania wielopoziomowych uprawnień
19. System powinien zapewniać możliwość monitorowania minimum 100.000 obiektów w ramach jednej instancji

**5.3 Wymagane prace wdrożeniowe**

1. instalacja przez oferenta rozwiązania na dedykowanym zasobie wirtualnym Zamawiającego;
2. konfiguracja wstępna i nadanie dostępów do logowania dla Zamawiającego;
3. przygotowanie po konsultacji z Zamawiającym monitoringu dla 10 urządzeń wytypowanych przez Zamawiającego (serwery, przełączniki, urządzenie brzegowe klasy UTM);
4. konfiguracja progów alarmów zgodnie z wymogami Zamawiającego oraz po konsultacji z Wykonawcą i wdrożeniem w oparciu o najlepsze praktyki;
5. konfiguracja powiadomień na wskazaną przez Zmawiającego skrzynkę pocztową za pośrednictwem dedykowanej skrzynce technicznej dostarczonej przez Zamawiającego.

**Część 6**

**Szkolenia z zakresu rozwiązań technicznych**

**6.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. Przeprowadzenie szkolenia z zakresu rozwiązań technicznych takich jak: Microsoft Active Directory, rozwiązania Fortinet Fortigate, Rozwiązań kopii zapasowych dedykowanych środowiskom zwirtualizowanym, bezpieczeństwa sieci

**6.2 Termin realizacji zamówienia**

Zamawiający wymaga, aby świadczenie szkoleń z zakresu rozwiązań technicznych, o której mowa w pkt 6.1 trwała w terminie 3 miesięcy od dnia zawarcia umowy.

**6.3 Szczegółowe wymagania odnośnie usługi**

1. Szkolenie - minimalne wymagania:
	1. szkolenia będą zrealizowane jako szkolenia zamknięte;
	2. szkolenia będą przeprowadzone w języku polskim;
	3. szkolenia muszą odbyć się w formie zdalnej poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego;
	4. musi tworzyć cykl szkoleń online trwających minimum 1 godzinę każde, gdzie łączna liczba godzin poświęcona na szkolenia nie może być mniejsza niż 25 godzin
	5. Zamawiający dopuszcza udział uczestników szkolenia w ramach większej grupy szkoleniowej
	6. agenda szkoleń musi dotykać tematyki technologicznej, w tym przynajmniej: usługi katalogowej wdrożonej, rozwiązania urządzeń sieciowych, Rozwiązań kopii zapasowych dedykowanych środowiskom zwirtualizowanym, bezpieczeństwa sieci
	7. obowiązek sprawdzania obecności w trakcie każdego ze szkoleń np. w postaci zrzutów ekranowych listy zalogowanych uczestników szkolenia pozwalającej potwierdzić obecność uczestników. Oryginalne wersje list obecności zostaną przekazane Zamawiającemu po zakończeniu każdej edycji szkolenia;
	8. wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, co najmniej na poziomie wymaganym do realizacji szkoleń;
	9. wykonawca jest zobowiązany przeprowadzić szkolenie w oparciu o zaakceptowane przez Zamawiającego materiały dydaktyczne;
	10. wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń. Zamawiający ustali na zasadzie negocjacji z Wykonawcą, w terminie maksymalnie 10 dni od daty podpisania umowy ramowy harmonogram szkoleń;
	11. po ukończeniu szkolenia uczestnicy otrzymają zaświadczenie lub certyfikat ukończenia szkolenia w formie papierowej bądź elektronicznej. Zaświadczenia zostaną przesłane na wskazany przez Zamawiającego adres fizyczny lub adres skrzynki poczty elektronicznej.

**Część 7**

**Dostarczenie i wdrożenie urządzenia UTM klasy NGF**

**7.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach;
2. konfiguracja, instalacja w szafie rakowej oraz wdrożenie rozwiązania w infrastrukturze Zamawiającego;
3. Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall;
* ochrony w warstwie aplikacji;
* protokołów routingu dynamicznego.

**7.2 Termin realizacji zamówienia**

Zamawiający wymaga, aby dostawa sprzętu, konfiguracja o którym mowa w pkt 7.1 do Zamawiającego nastąpiła w terminie 7 dni od dnia zawarcia Umowy.

**7.3 Wymagania szczegółowe odnośnie sprzętu:**

1. Redundancja, monitoring i wykrywanie awarii:
	1. w przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall;
	2. monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych;
	3. monitoring stanu realizowanych połączeń VPN;
	4. system musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
2. Interfejsy, dysk zasilanie:
3. System realizujący funkcję Firewall musi dysponować minimum:
* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC bezpośrednie lub poprzez zasilacz sieciowy
4. Parametry wydajnościowe:
5. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
6. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
7. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
8. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
9. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
10. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
11. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
12. Funkcje systemu bezpieczeństwa

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Analiza ruchu szyfrowanego protokołem SSH.
13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
14. Polityki i Firewall:
15. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
16. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
	* 1. Translację jeden do jeden oraz jeden do wielu.
		2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
17. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
18. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
19. Połączenia VPN
	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
		1. Wsparcie dla IKE v1 oraz v2.
		2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
		3. Obsługa protokołu Diffie-Hellman grup 19 i 20.
		4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
		5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
		6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
		7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
		8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
		9. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
	2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
		1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
		2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
		3. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
20. Routing i obsługa łączy WAN:
	1. w zakresie routingu rozwiązanie powinno zapewniać obsługę:
		1. routingu statycznego;
		2. policy Based Routingu;
		3. protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
21. Funkcje SD-WAN:
	1. system powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN;
	2. reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
22. Zarządzanie pasmem:
	1. system Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu;
	2. musi istnieć możliwość określania pasma dla poszczególnych aplikacji;
	3. system musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
23. Ochrona przed malware
	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
	2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
	3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych.
	4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
	5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
	6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
24. Ochrona przed atakami:
	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
	2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
	3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
	4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
	5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
	6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
	7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
25. Kontrola aplikacji:
	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
	2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
	3. Aplikacje chmurowe powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
	4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
	5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
26. Kontrola WWW:
	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
	2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
	3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Filtr WWW musi dostarczać kategorie które można rozbudowywać stron zabronionych.
	4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
	5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek.
	6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
	7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
27. Uwierzytelnianie użytkowników w ramach sesji:
	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
		1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
		2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
		3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
	2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
	3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
	4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
28. Zarządzanie:
	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
	2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
	3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
	4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
	5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
	6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
	7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
29. Logowanie:
	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
	2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
	3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
	4. Musi istnieć możliwość logowania do serwera SYSLOG.
30. Certyfikaty:
	1. poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.
31. Serwisy i licencje:

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

* 1. kontrola Aplikacji
	2. IPS
	3. Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych)
	4. Analiza typu Sandbox
	5. Antyspam
	6. Web Filtering
	7. bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
1. Gwarancja oraz wsparcie:
	1. system musi być objęty serwisem gwarancyjnym producenta przez okres min. 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**7.4 Wymagane prace wdrożeniowe:**

1. dostarczenie fabrycznie nowego sprzętu;
2. instalacja sprzętu we wskazanej szafie rack;
3. podłączenie sprzętu do instalacji elektrycznej;
4. podłączenie sprzętu do infrastruktury sieciowej Zamawiającego we wskazane porty;
5. wstępna konfiguracja urządzenia polegająca na aktualizacji firmware’u do możliwie jak najwyższej i stabilnej wersji oprogramowania;
6. utworzenie kont dostępowych dla dostępu administracyjnego do urządzenia;
7. konfiguracja polityk bezpieczeństwa w zakresie ograniczenia ruchu z i do sieci Zamawiającego w oparciu o najlepsze praktyki i wytyczne zamawiającego;
8. przeniesienie konfiguracji z obecnego urządzenia zainstalowanego u Zamawiającego

**Część 8**

**Modernizacja infrastruktury sieciowej**

**8.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach, w ilościach:
	1. Przełącznik sieciowy min. 48 port – 3 sztuki
2. konfiguracja urządzeń oraz fizyczna instalacja w infrastrukturze IT Zamawiającego;
3. udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
4. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;

**8.2 Termin realizacji zamówienia oraz liczba dostarczanego sprzętu**

Zamawiający wymaga, aby dostawa sprzętu, o którym mowa w pkt 8.1 do Zamawiającego nastąpiła w terminie 7 dni od dnia zawarcia Umowy.

**8.3 Wymagania szczegółowe Zamawiającego**

**Zestawienie wymaganych parametrów technicznych dla przełączka sieciowego (3 sztuki)**

|  |  |
| --- | --- |
| Interfejs sieciowy | 48x 1Gb Ethernet (10/100/1000 Mbps)4x SFP+ (1/10 Gbps) |
| Interfejs zarządzania | Ethernet, In-Band |
| Łączna przepustowość (non-blocking) | Minimum 88 Gbps |
| Przepustowość przełączania | Minimum 176 Gbps |
| Prędkość przekazywania | Minimum 130 Mpps |
| Sposób zasilania | Uniwersalny: 100 - 240 V AC / 50 - 60 HzUSP RPS DC: 52VDC, 11.54A; 11.5VDC, 5.22A |
| Zasilacz | Wbudowany, AC/DCMoc minimum 650 W |
| Maksymalny pobór mocy | Bez zasilania PoE: maksymalnie 60 W |
| Diody LED | System: StatusRJ45: PoE; Speed / Link / ActivitySFP+: Link / Activity |
| Waga | Z uchwytami montażowymi: maksymalnie 6,40 kgBez uchwytów montażowych: maksymalnie 6,30 kg |
| Dopuszczalna temperatura pracy | Od -5 do 40 st. C |
| Certyfikaty | IC, FCC, CE |
| Możliwość montażu w szafie RACK | Tak, maksymalnie 1U |
| **PoE** |
| Interfejsy | 40 x PoE+ IEEE 802.3af/at8 x 60W PoE++ IEEE 802.3af/at/bt |
| Maksymalny budżet PoE | 600 W |
| Maksymalna moc PoE | Dla 802.3at: minimum 30 WDla 802.3bt: minimum 62W |
| Zakres napięcia | Dla 802.3af: 44-57 VDla 802.3at/bt: 50-57 V |
|  |  |

**8.4 Wymagania ogólne dla przełączników sieciowych oraz wykonywanych prac:**

1. Dostarczone urządzenia muszą pochodzić z autoryzowanego kanały sprzedaży producentów na rynek polski – do oferty należy dołączyć odpowiednie oświadczenie producenta sprzętu
2. Dostarczone urządzenia muszą być objęte gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależnie od statusu partnerskiego Wykonawcy przez okres co najmniej 36 miesięcy.
3. Urządzenie musi mieć możliwość zarządzania i konfigurowania poprzez dedykowane rozwiązanie zarządzające, posiadające funkcje takie jak:
	1. podgląd statusu urządzeń w czasie rzeczywistym
	2. centralne zarządzanie wieloma sieciami z poziomu interfejsu graficznego
	3. możliwość zdalnej aktualizacji oprogramowania urządzeń
	4. wersję mobilną aplikacji
4. Urządzenie musi być zarządzalne w warstwie 2 i 3
5. Wykonawca jest zobowiązany do podłączenia urządzeń sieciowych w infrastrukturze Zamawiającego do wskazanych miejsc połączeń sieciowych i elektrycznych
6. Wykonawca jest zobowiązany do aktualizacji oprogramowania sprzętowego dostarczonych urządzeń do najnowsze dostępnej i zalecanej przez producenta wersji
7. Wykonawca musi utworzyć dostępy administracyjne do urządzeń oraz przekazać je Zamawiającemu
8. W ramach przekazanych urządzeń, Wykonawca zobowiązuje się - na wskazanych przez Zamawiającego interfejsach - zdefiniować sieć do 4 VLAN-ów
9. Na wskazanym przez Zamawiającego zasobie wirtualnym serwera, Wykonawca zobowiązany jest do instalacji, konfiguracji i dodania urządzeń sieciowych do dedykowanego centralnego rozwiązania zarządzającego

**Część 9**

**Szkolenia z zakresu cyberbezpieczeństwa**

**9.1 Przedmiot zamówienia**

 Przedmiotem zamówienia jest:

1. przeprowadzenie szkolenia zwiększającego świadomość pracowników Zamawiającego w dziedzinie cyberbezpieczeństwa;

**9.2 Termin realizacji zamówienia**

Zamawiający wymaga, aby przedmiot, o którym mowa w pkt 9.1 cykl szkoleń odbył się w terminie 3 miesięcy od dnia zawarcia umowy.

**9.3 Szczegółowe wymagania odnośnie usługi**

1. Szkolenie - minimalne wymagania:
	1. szkolenia będą zrealizowane jako szkolenia zamknięte;
	2. szkolenia będą przeprowadzone w języku polskim;
	3. szkolenia muszą odbyć się w formie zdalnej poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego;
	4. szkolenie musi trwać min. 5 godzin.
	5. Zamawiający dopuszcza udział uczestników szkolenia w ramach większej grupy szkoleniowej pracowników Urzędu Miejskiego w Sępólnie Krajeńskim;
	6. agenda szkoleń musi dotykać tematyki cyberbezpieczeństwa, w tym przynajmniej: socjotechniki, phishingu, ransomware, bezpieczeństwa poczty elektronicznej oraz korzystania z urządzeń mobilnych, sieci Wi-Fi, bezpieczeństwa nośników danych;
	7. obowiązek sprawdzania obecności w trakcie każdego ze szkoleń np. w postaci zrzutów ekranowych listy zalogowanych uczestników szkolenia pozwalającej potwierdzić obecność uczestników. Oryginalne wersje list obecności zostaną przekazane Zamawiającemu po zakończeniu każdej edycji szkolenia;
	8. wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, co najmniej na poziomie wymaganym do realizacji szkoleń;
	9. wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń. Zamawiający ustali na zasadzie negocjacji z Wykonawcą, w terminie 10 dni od daty podpisania umowy ramowy harmonogram szkoleń;
	10. po ukończeniu szkolenia uczestnicy otrzymają zaświadczenie lub certyfikat ukończenia szkolenia w formie papierowej. Zaświadczenia zostaną przesłane na adres Urzędu Miejskiego w Sępólnie Krajeńskim.

**Część 10**

**Dostarczenie stacji roboczych**

**10.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach
	1. Komputer stacjonarny typu All-in-One – 5 sztuk
	2. Komputer typu Notebook – 2 sztuki

**10.2 Termin realizacji zamówienia oraz liczba dostarczanego sprzętu**

Zamawiający wymaga, aby dostawa sprzętu, o którym mowa w pkt 10.1 do Zamawiającego nastąpiła w terminie 7 dni od dnia zawarcia Umowy.

**10.3 Wymagania szczegółowe Zamawiającego**

**Zestawienie wymaganych parametrów technicznych Komputer stacjonarny typu All-in-One – 5 sztuk:**

|  |  |
| --- | --- |
| Przekątna ekranu | Min 23,5" |
| Rozdzielczość | Min. 1920 x 1080 |
| Typ matrycy | TFT WVA |
| Powierzchnia matrycy | Matowa |
| Taktowanie procesora | 2.3 GHz |
| Taktowanie (Boost) | 3.8 GHz |
| Zainstalowana pamięć RAM | 8 GB |
| Maks. wielkość pamięci | 64 GB |
| Rodzaj pamięci | DDR4 |
| Częstotliwość szyny pamięci | 2666 MHz |
| Typ dysku | SSD |
| Pojemność SSD | Min. 256 GB |
| Format szerokości SSD | M.2 |
| Interfejs dysku SSD | PCI-Express |
| Rodzaj karty graficznej | Zintegrowana |
| Porty wideo | 1 x DisplayPort |
| Interfejs sieciowy | * 1 x 10/100/1000 Mbit/s
* Wi-Fi 802.11a/b/g/n/ac/ax
* Bluetooth
 |
| Czytnik kart pamięci | Tak |
| Porty USB | * 2 x USB 2.0 Type-A
* 3 x USB 3.0 Type-A
* 1 x USB 3.1 Type-C
 |
| Pozostałe porty we/wy | * 1 x Audio (Line-out)
* 1 x RJ-45
 |
| Kamera internetowa | Tak |
| Mikrofon | Tak |
| Obudowa | All-In-One |
|  System operacyjny | Najnowszy system w wersji 64 bitowej obsługujący Active Directory oraz współdziałający z istniejącymi systemami używanymi w Urzędzie Miejskim W Sępólnie KrajeńskimSystem operacyjny ma być zainstalowany na dostarczonym Sprzęcie. * Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim,
* Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
* Wbudowany system pomocy w języku polskim,
* Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
* Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
* Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
* Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
* Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
* Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
* Możliwość zabezpieczenia hasłem dostępu do systemu,
* Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych)
* Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
* Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
* Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
* Możliwość pracy na kilu zdalnych pulpitach
 |
| Pakiet aplikacji biurowych | Najnowszy w architekturze x64 arkusz kalkulacyjny, edytor tekstu, program do obsługi poczty, program do tworzenia prezentacji multimedialnych współpracujący z oprogramowaniem użytkowym wykorzystywanym w Urzędzie Miejskim w Sępólnie Krajeńskim, automatyczne aktualizacje oprogramowania biurowego |
| Akcesoria w zestawie | * Klawiatura w układzie polskim
* Mysz optyczna
 |
| Informacje o gwarancji | Minimum 36 miesięcy |

**Zestawienie wymaganych parametrów technicznych Komputer typu Notebook – 2 sztuki**

|  |  |
| --- | --- |
| Taktowanie procesora | 2.4 GHz |
| Taktowanie (Boost) | 4.2 GHz |
| Przekątna ekranu | 15,6'' |
| Rozdzielczość | 1920 x 1080 |
| Powierzchnia matrycy | Matowa |
| Technologia podświetlania | Diody LED |
| Rodzaj karty graficznej | Zintegrowana |
| Zainstalowana pamięć RAM | 8 GB |
| Maks. wielkość pamięci | 16 GB |
| Rodzaj pamięci | SODIMM DDR4 |
| Częstotliwość szyny pamięci | 2666 MHz |
| Typ dysku | SSD |
| Pojemność SSD | 512 GB |
| Format szerokości SSD | M.2 |
| Interfejs dysku SSD | PCI-Express |
| Komunikacja | * LAN 10/100/1000
* WiFi 802.11 ax
* Bluetooth
 |
| Porty USB | * 1 x USB 2.0 Type-A
* 2 x USB 3.1 Type-A
 |
| Porty wideo | 1 x HDMI |
| Czytnik kart pamięci | Tak |
| Pozostałe porty we/wy | * 1 x Audio (Słuchawki / Line-out)
* 1 x Audio (Mikrofon)
* 1 x RJ-45
 |
| Kamera internetowa | Tak |
| Mikrofon | Tak |
| Podświetlana klawiatura | Tak |
| Czytnik linii papilarnych | Tak |
| System operacyjny | Najnowszy system w wersji 64 bitowej obsługujący Active Directory oraz współdziałający z istniejącymi systemami używanymi w Urzędzie Miejskim w Sępólnie KrajeńskimSystem operacyjny ma być zainstalowany na dostarczonym Sprzęcie. * Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim,
* Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
* Wbudowany system pomocy w języku polskim,
* Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
* Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
* Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
* Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
* Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
* Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
* Możliwość zabezpieczenia hasłem dostępu do systemu,
* Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych)
* Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
* Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
* Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),

Możliwość pracy na kilu zdalnych pulpitach  |
| Pakiet aplikacji biurowych | Najnowszy w architekturze x64 arkusz kalkulacyjny, edytor tekstu, program do obsługi poczty, program do tworzenia prezentacji multimedialnych współpracujący z oprogramowaniem użytkowym wykorzystywanym w Urzędzie Miejskim w Sępólnie Krajeńskim, automatyczne aktualizacje oprogramowania biurowego  |
| Waga | Maksymalnie 1.75 kg |
| Akcesoria w zestawie | * Zasilacz
* Europejski przewód zasilający
 |
| Informacje o gwarancji | Minimum 36 miesięcy |

**Część 11**

**Wykonanie usługi polegającej na zaprojektowaniu, utworzeniu i świadczeniu usługi chmurowej w postaci serwisu www dla Gminy Sępólno Krajeńskie**

**Przedmiot zamówienia:**

Wykonania usługi polegającej na zaprojektowaniu, utworzeniu i świadczeniu usługi chmurowej w postaci serwisu www dla Gminy Sępólno Krajeńskie, zarchiwizowanie obecnej strony www, skonfigurowanie obecnego hostingu.

**Termin realizacji:**

Zamawiający wymaga, aby uruchomienie strony Zamawiającego nastąpiło w terminie 6 tygodni od dnia zawarcia umowy.

1. **Wymagania dla projektu graficznego usługi chmurowej – serwisu www.**
2. Projekt serwisu www musi uwzględniać zasady UI oraz UX, a także WCAG 2.1 dla całego układu serwisu www oraz rozmieszczenia elementów, jak również w kwestii zastosowanych czcionek, kontrastu elementów graficznych oraz tła itp.
3. Projekt graficzny serwisu www musi być opracowany dla różnego rodzaju wielkości ekranów, aby zapewnić responsywność.
4. Rozdzielczość dla wersji desktop szerokość wyświetlanego kontentu to 1600px, ale całość serwisu wyświetlana jest na 100% ekranu.
5. Zastosowany kontrast zgodny z wytycznymi dotyczącymi dostępności treści cyfrowych (WCAG 2.1). Współczynnik kontrastu co najmniej 4,5:1 dla zwykłego tekstu i 3:1 dla dużego tekstu (co najmniej 18 punktów) lub tekstu pogrubionego.
6. Projekt powinien zapewnić dostęp do najważniejszych informacji serwisu www, w jak najmniejszej ilości kliknięć – preferowane są max 3 kliknięcia.
7. Projekt graficzny musi być tak zaprojektowany, aby była możliwość tworzenia różnych konfiguracji układu strony głównej, bazując na układzie uzgodnionym z zamawiającym. Realizacja tej funkcjonalności powinna być możliwa poprzez np. zmianę kolejności poszczególnych sekcji na stronie głównej, włączanie i wyłączanie modułów funkcjonalnych, zachowując przy tym zasady UI/UX, WCAG 2.1 oraz walory estetyczne, tak aby nie powstawały puste niewykorzystane przestrzenie na stronie głównej serwisu www.
8. Dobór kolorystyki serwisu www, projekt strony będzie uzgodniony z Zamawiającym.
9. Projekt graficzny musi być wykonany w oparciu o wizualizację/makietę układu sekcji i modułów strony głównej serwisu www oraz przykładowych podstron. Przykład obecna strona www.gmina-sepolno.pl
10. Proces projektowy serwisu www uwzględniać będzie również przygotowanie wersji żałobnej, narodowej oraz świątecznej serwisu www.
11. Wykonawca uzgodni z Zamawiającym koncepcję strony www w ciągu 7 dni od dnia zawarcia umowy.
12. **Wymagania funkcjonalne dla usługi chmurowej –  Portal www będzie posiadał  maksymalnie następujące funkcjonalności, które mogą być uruchomione lub nie, w zależności od potrzeb:**
13. slider aktualności, z możliwością wyłączenia przez Internautę automatycznego przesuwania się kolejnych aktualności
14. aktualności, w tym możliwość implementowania aktualności z jednego serwisu www np. Urzędu Miejskiego do innego serwisu www np. gminnych jednostek organizacyjnych i odwrotnie – funkcjonalność moderowana; możliwość kategoryzacji aktualności np. Sportowe, Kulturalne itp.; integracja aktualności z modułem Galeria oraz Kalendarz wydarzeń
15. kalendarz wydarzeń zintegrowany z aktualnościami,
16. galerie zdjęć z możliwością ich przeglądania: zdjęcie następne, zdjęcie poprzednie, możliwość podpisania każdego zdjęcia z osobna oraz wszystkich poprzez np. skrypt , możliwość dodania do jednej galerii max. 300 zdjęć, możliwość z miniaturki zdjęcia powiększenia go, dodawanie zdjęć na zasadzie np. Jak na Facebook’u
17. ruchomy pasek aktualności, z możliwością wyłączenia przez Internautę,
18. slider plakatów, z możliwością wyłączenia, automatycznego przesuwania się przez Internautę,
19. system banerowy,
20. pop up, z możliwością wyłączenia przez Internautę,
21. sondę,
22. mapa serwisu odzwierciedlającą widoczne elementy struktury serwisu,
23. integracja z walidatorem Wave WCAG 2.1,
24. newsletter wraz z systemem e-mail marketing,
25. powiadomienia Web Push dla aktualności, z możliwością ich wysyłki w ramach panelu zarządzania,
26. dzień tygodnia i pogodę,
27. zadaj pytanie do,
28. katalog firm i instytucji
29. wykaz/katalog spraw urzędowych
30. statystyki odwiedzin zintegrowane z Google Analytics,
31. funkcja strony do druku dla każdej informacji tekstowej, dostępna poprzez ikonkę pod każdą informacją,
32. funkcja udostępnienia informacji na profilu Facebook, dla każdej informacji tekstowej, dostępna poprzez ikonkę pod każdą informacją,
33. wyszukiwarka,
34. formularz kontaktowy,
35. formularz zapisu do newslettera
36. formularz zapisu do powiadmień WebPush
37. kanał RSS,
38. deklaracja dostępności,
39. wersja serwisu www w wysokim kontraście,
40. powiększanie/pomniejszanie czcionki/ zwiększanie odstępów pomiędzy znakami i wersami tekstu,
41. informacja o miejscu w strukturze serwisu internetowego, w którym znajduje się aktualnie internauta, tzw. ścieżka dostępu, breadcrumbs
42. Archiwum starej strony
43. Możliwość dodawania linków do strony YouTube (dodanie nie odnośnika- hiperłacza do Youtube tylko umieszczenie materiału z YT jako na stronie)
44. Dodawanie materiałów w plikach np. mp3, mp4 itp….
45. Strona ma być wielojęzyczna np. Angielski, Niemiecki, Ukraiński – translator google.
46. **Wymagania dotyczące systemu CMS do zarządzania usługą chmurową - serwisem www dostępne w panelu zarządzania:**
47. panel administracyjny w polskiej wersji językowej,
48. system CMS musi posiadać mechanizm przekierowujący użytkownika na zaprojektowaną przez Dostawcę stronę informacji o błędzie (ERROR 404) w przypadku podania niewłaściwego adresu strony WWW, na której znajdzie się informacja o braku szukanego adresu oraz link do strony głównej danej strony WWW,
49. dostęp do panelu administracyjnego powinien być możliwy poprzez wejście na konkretny adres strony www,  za pomocą loginu i hasła, zaszyfrowany za pomocą certyfikatu SSL,  logowanie dwuetapowe np. Google authenticator
50. system CMS dostarczony przez Dostawcę musi umożliwiać zarządzanie treścią całego serwisu internetowego bez konieczności znajomości języków programowania (do obsługi ma być wystarczająca podstawowa znajomość programów do edycji tekstu, obróbki grafiki).
51. system CMS musi obsługiwać wszystkie strony serwisu internetowego oraz wszystkie bazy, rejestry, listy etc.
52. pełne zarządzanie menu, tzn. dodawanie/usuwanie zakładek i podzakładek, możliwość stworzenia minimum 3 poziomów struktury menu,
53. tworzenie linków między zakładkami i podzakładkami,
54. budowanie hierarchii menu, w tym struktury, która pozostaje nie widoczna na stronie prezentacyjnej,
55. możliwość zmiany umiejscowienia elementów struktury menu, w tym kolejności wyświetlania oraz przenoszenia poszczególnych elementów np. podstrony jako stronę, lub odwrotnie, przyporządkowanie danej strony lub podstrony pod inny dział, stronę itd.
56. możliwość tworzenia różnych konfiguracji układu strony głównej, bazując na tym samym układzie zgodnie z załącznikiem do specyfikacji.  Realizacja tej funkcjonalności powinna być możliwa poprzez np. zmianę kolejności poszczególnych sekcji strony głównej, włączanie i wyłączanie modułów funkcjonalnych, zachowując przy tym zasady UI/UX, WCAG 2.1 oraz walory estetyczne, tak aby nie powstawały puste niewykorzystane przestrzenie na stronie głównej serwisu www.
57. zarządzanie widocznością  i publikacją elementów struktury,
58. możliwość podejrzenia tworzonej treści bez jej publikacji na stronie wynikowej,
59. możliwość włączenia i wyłączenia graficznej wersji żałobnej, narodowej i świątecznej serwisu,
60. łatwa, pełna edycja tekstu za pomocą WYSIWYG, w tym z możliwością:
61. pogrubienia, kursywy, podkreślenia tekstu,
62. wyrównania tekstu, zdjęcia, tabelki: do lewej, do środka, do prawej, równaj do prawej i lewej,
63. skorzystania z wbudowanych styli: nagłówki od 1 do 6
64. skorzystania z listy wbudowanych rodzajów czcionek,
65. określenia wielkości czcionki w danym tekście,
66. określenia koloru czcionki oraz koloru tła pod tekstem,
67. kopiowania, wycinania i wklejania podczas edycji treści,
68. wklejania treści z edytorów tekstu np. z MS Word,
69. zastosowania listy numerowanej i punktowanej,
70. zastosowania wcięcia, cofnięcia wcięcia,
71. cofnięcia i ponowienia operacji,
72. wstawienia i edytowania linków do: pliku, zdjęcia, adresu email, strony www – z określeniem czy w tym samym oknie, czy w nowym,
	1. wstawienia pliku graficznego w treści za pomocą przeglądaj dysk, z możliwością
		1. określenia tytułu pliku oraz opisu alternatywnego,
		2. określenia pozycji zdjęcia względem tekstu (wyrównanie do lewej lub prawej, oblanie tekstem, pozycja zdjęcia względem tekstu)
		3. wstawienie ramki z określeniem jej grubości,
	2. przełączenia się w tryb HTML,
	3. wstawienia filmu lub pliku audio,
	4. wstawienia tabeli z możliwością:
		1. ustawienia liczby kolumn i wierszy
		2. określenia odległości komórek od siebie,
		3. określenia zawartości komórki od jej ramki,
		4. wyrównanie tabeli względem tekstu,
		5. określenie obramowania tabeli,
		6. szerokości i wysokości
		7. kolor ramki i kolor tła,
	5. możliwość ustawienia odstępu powyżej i poniżej wiersza,
	6. możliwość implementacji ramki iframe z różnych źródeł zawierającej np. plik audio, video, kod html
73. dodawanie załączników, do każdej podstrony tekstowej struktury serwisu, załączony załącznik musi być  prezentowany w sposób automatyczny na stronie wynikowej (bez potrzeby ingerencji osoby redagującej), zgodnie z wymogami WCAG 2.1 tj. muszą posiadać nazwę pliku, rozmiar i typ,
74. każdy plik graficzny implementowany do zawartości serwisu www musi posiadać możliwość przy jego dodawaniu, określenia jego tytułu, opisu alternatywnego za pomocą odpowiednich pól,
75. funkcjonalność umożliwiająca zarządzanie aktualnościami:
	1. zarządzanie aktualnością – dodawanie nowej, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
	2. możliwość dodawania kategorii aktualności: np. dla biznesu, finansowe, itp.
	3. wypromowanie artykułu w sliderze (pole rozpoczęcia publikacji, zakończenia publikacji danego artykułu od strony zaplecza)
	4. dodanie danego artykułu również do kalendarza wydarzeń,
	5. możliwość podpięcia galerii, która nie jest widoczna na stronie głównej
	6. możliwość umieszczenia wybranych aktualności z jednego serwisu www w  innych serwisach www i odwrotnie (serwisach www powstałych w  wyniku tego postępowania, zbudowanych o tę samą technologię), moduł moderowany – użytkownik z odpowiednimi uprawnieniami decyduje czy opublikować daną aktualność w swoim serwisie www.
	7. załączanie plików, w tym:
		1. implementacja plików graficznych w tekście, które muszą posiadać możliwość kadrowania, obracania, powiększania i pomniejszania, tzw. ustawienia oblewania tekstem oraz obok tekstu z lewej i prawej – w celu uzyskania odpowiedniej kompozycji,
		2. załączane pozostałe pliki jako załączniki – muszą być prezentowany w sposób automatyczny na stronie wynikowej (bez potrzeby ingerencji osoby redagującej), zgodnie z wymogami WCAG 2.1 tj. muszą posiadać nazwę pliku, rozmiar i typ,
76. funkcjonalność umożliwiająca zrządzanie galerią zdjęć:
	1. zarządzanie galerią – dodawanie nowej, edycja i usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
	2. dodawanie zdjęć potokowo(czyli dużej ilości plików jednorazowo) za pomocą technologii Drag& Drop,
	3. dodawanie zdjęć potokowo za pomocą opcji przeglądaj z dysku,
	4. dodawanie pojedyncze zdjęć,
	5. określenie nazwy dodawanych zdjęć lub nadanie im nazwy z danej galerii,
	6. automatyczną kompresję plików o dużej pojemności i dostosowywanie ich do optymalnych cech (rozmiar w px, pojemność w MB),  w celu ich poprawnej publikacji ze względu na wysokość ekranu i szybkości ładowania na stronie www,
	7. przeglądanie zdjęć za pomocą wbudowanej przeglądarki, prezentującej zdjęcia na warstwie, umożliwiającej przechodzenie do następnego zdjęcia oraz poprzedniego, a także zamykanie okna.
77. funkcjonalność umożliwiająca zrządzanie kalendarzem wydarzeń:
	1. zarządzanie wydarzeniem – dodawanie nowego, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
	2. ustawienie nazwy wydarzenia,
	3. ustawienie daty wydarzenia,
	4. ustawienie od kiedy do kiedy dane wydarzenie ma trwać,
	5. ustawienie od kiedy do kiedy dane wydarzenie ma być widoczne w kalendarzu,
78. funkcjonalność umożliwiająca zrządzanie ruchomym paskiem informacyjnym:
	1. zarządzanie  – dodawanie nowej informacji, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
	2. ustawienie tytułu informacji,
	3. ustawienie daty informacji,
	4. zlinkowanie do strony zewnętrznej lub elementu struktury serwisu www,
	5. możliwość przypisania galerii,
79. funkcjonalność umożliwiająca zrządzanie banerami w określonych miejscach serwisu www np. polecamy, na skróty, zdjęcia w top, zdjęcie dla modułu statystycznego:
	1. zarządzanie banerami - dodawanie nowego, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
	2. tworzenie pop-up na warstwie,
	3. możliwość linkowania do stron zewnętrznych oraz podstron serwisu,
	4. slider plakatów – funkcjonalność umożliwiająca prezentację plików w formacie pionowym,
80. funkcjonalność umożliwiająca zrządzanie sondą:
	1. zarządzanie sondą - dodawanie nowego, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
	2. tworzenie pytania,
	3. tworzenie nagłówka sondy,
	4. ustawienia opcji głosowania: wielokrotne, jednokrotne,
	5. widoczność sondy od ..do,
	6. widoczność wyników głosowania tak/nie,
81. funkcjonalność umożliwiająca zarządzanie – zadaj pytanie:
	1. Zarządzanie listą osób/stanowisk do których można zadać pytanie poprzez formularz „Zadaj pytanie” : niezbędne pola: Imię i Nazwisko lub Stanowisko, adres email, widoczność, pozycja – kolejność osób na liście, usuń/edytuj, dodaj;
82. funkcjonalność umożliwiająca zarządzanie – katalogiem firm i instytucji
	1. Dodawanie kategorii w biznesie lub rodzaju instytucji np. Apteki, Lekarze, Hotele itp.
	2. Możliwość dodawania wpisu do katalogu przez redaktora lub internautę, z podaniem nazwy i danych adresowych danego podmiotu, wyborem branży, krótkim opisem i zdjęciem, adres www, email kontaktowy, wymagane podanie adresu email i telefonu dla dodającego internauty,
	3. Moduł moderowany – redaktor weryfikuje i decyduje które wpisy będą wyświetlane i w jakiej formie i kategorii.
83. funkcjonalność umożliwiająca zarządzanie – wykazem spraw:
	1. dodawanie/edycja kategorii spraw np. Podatek od nieruchomości
	2. dodawanie/edycja wydziałów/stanowisk
	3. dodawania/edycja karty sprawy według opracowanego szablonu,
84. newsletter wraz z systemem e-mail marketing, z możliwością:
	1. skonfigurowania konta do wysyłki newsletterów bez użycia zewnętrznego programu pocztowego,
	2. tworzenia wiadomości do wysłania za pomocą newslettera, w tym z załącznikami, z automatycznym linkiem do rezygnacji z prenumeraty oraz innym zaprojektowanym tekstem,
	3. tworzenie i zarządzanie szablonów wiadomości  w tym co najmniej:
		1. wiadomości usunięcia konta,
		2. wiadomość powitalna po aktywacji,
		3. wiadomość aktywacji konta,
	4. tworzenia kopii roboczych wiadomości,
	5. tworzenia i zarządzania grupami mailingowymi,
	6. przechowywania wiadomości do wysyłki w skrzynce nadawczej z następującymi funkcjami:
		1. w przypadku zamknięcia skrzynki nadawczej w trakcie wysyłania np. wylogowanie się, brak prądu – wysyłka zostaje przerwana, a nie anulowana,
		2. ponowne otwarcie skrzynki nadawczej kontynuuje wysyłkę od momentu w jakim została przerwana,
		3. w trakcie wysyłki mailingu można zatrzymać proces,
		4. podczas wysyłki mailingu, na bieżąco podawana jest informacja o ilości wysyłanych wiadomości,
	7. przechowywania wysłanych wiadomości w elementach wysłanych, w tym z informacjami :
		1. do ilu adresatów wysłano mailing,
		2. o ilości kliknięć w odnośniki (linki) w wiadomości- wartość liczbowa,
		3. o ilości kliknięć w odnośniki (linki) w wiadomości- wartość procentowa,
		4. o ilości otwarć (odczytu) wiadomości – wartość liczbowa,
		5. o ilości otwarć (odczytu) wiadomości – wartość procentowa,
		6. o dacie wysyłki,
	8. przetestowania poprawności wysyłki oraz struktury wysyłanej wiadomości na określone adresy email,
	9. zarządzania adresami email, w tym z możliwością
		1. usuwania i dodawania adresów ręcznie,
		2. importu adresów email z pliku csv, w tym z możliwością:
			1. automatycznego aktywowania importowanych adresów email,
			2. pominięcia  adresów email, które występują w innych grupach mailingowych,
		3. podglądem statusu adresu email – czy jest aktywny czy nieaktywny,
		4. usuwaniem z bazy zaznaczonych adresów,
		5. subskrybowaniem zaznaczonych adresów,
		6. wypisaniem zaznaczonych adresów,
		7. przypisaniem i dodaniem zaznaczonych adresów do grup,
		8. aktywowanie i deaktywowanie zaznaczonych adresów,
		9. uzyskania informacji:
			1. adresie email,
			2. dacie dodanie adresu do bazy mailingowej,
			3. o adresie IP skąd nastąpiło dodanie adresu,
			4. ile wysłano wiadomości do tego adresu,
			5. ile było kliknięć w odnośniki w treści wiadomości przez użytkownika tego adresu,
			6. ile było otwarć wiadomości (odczytu) przez użytkownika adresu email
			7. do jakiej grupy przypisany jest adres email,
			8. status adresu: aktywny, nieaktywny, wypisany, niewypisany.
	10. przeszukiwania skrzynki po wysłaniu mailingu, w celu zidentyfikowania i usunięcia  emaili, generujących tzw. odbicia – czyli  adresów email, do których dana wiadomość nie dotarła,
	11. konfigurowania działania systemu newsletter w przypadku odbić twardych oraz miękkich, w tym co najmniej:
		1. w przypadku odbić twardych – konfiguracja komunikatów dotyczących przyczyny odbicia, zgodnie z systematyką komunikatów błędów poczty email; np. account not found, host not found,
		2. w przypadku odbić miękkich:
			1. konfiguracja komunikatów dotyczących przyczyny odbicia, zgodnie z systematyką komunikatów błędów poczty email; np. skrzynka przepełniona itp.
			2. konfiguracja ilości odbić miękkich, które przekształcą się w odbicie twarde: ile razy skrzynka musi odbić wiadomość
			3. konfiguracja ilość dni, w których odbicie miękkie jest ignorowane: przez ile dni wiadomość jest odrzucana,
85. funkcjonalność zarządzania użytkownikami systemu:
	1. lista użytkowników,
	2. dodawanie i zarządzanie użytkownikami,
	3. nadawanie uprawnień do poszczególnych modułów oraz funkcjonalności dla utworzonych grup,
	4. możliwość tworzenia i zarządzania grupami użytkowników np. administratorzy, redaktorzy – wraz z przydzieleniem ich dostępu do określonych modułów, funkcjonalności,
	5. możliwość odblokowywania zablokowanych użytkowników z powodu błędnego logowania,
86. funkcjonalność integracji z kontem Google Analytics w celu uzyskania szczegółowych statystyk odwiedzalności serwisu, w tym co najmniej:
	1. graficzne w formie wykresu i liczbowe, przedstawienie statystyk odwiedzalności, w podziale na godziny, dni, tygodnie oraz niestandardowy,  w tym zakres określonych dat,
	2. publikacja informacji o liczbie: sesji, użytkownikach, nowych użytkownikach, odsłonach, średnim czasie trwania sesji, strony/sesję,
87. funkcjonalność SEO – w celu określenia podstawowych danych serwisu, podlegających indeksowaniu przez wyszukiwarki internetowe, umożliwiająca co najmniej:
	1. określenie pola Title (tytuł),
	2. określenie pola Descryption (Opis),
	3. określenie keywords (słów kluczowych),
88. funkcjonalność konfiguracji kont email przeznaczonych do obsługi np. formularza kontaktowego, newslettera,
89. funkcjonalność tworzenia, udostępnienia i zarządzania deklaracją dostępności zgodnej ze wzorem opublikowanym przez właściwego Ministra, zgodnie z wymogami Ustawy o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych z dnia 4 kwietnia 2019 roku.
90. Funkcjonalność generowania raportów:
	1. Liczba subskrybentów usługi newsletter oraz zarządzanie adresami, import list mailingowych
	2. Zajętości miejsca na serwerze oraz ilość odwiedzin/wizyt w danym miesiącu
	3. Liczba otwarć i kliknięć dla wysłanych newsletterów
91. **Pozostałe wymagania dla usługi chmurowej - serwisu www.**
92. Wykonany serwis www powinien spełniać wymagania obowiązujących przepisów prawa.
93. Serwis internetowy musi być przygotowany w wersji responsywnej (automatyczne dopasowującej się rozdzielczości urządzeń na których jest przeglądana, a także do różnych przeglądarek internetowych).
94. Serwis internetowy musi  być przygotowany w technologii umożliwiającej korzystanie ze strony internetowej na urządzeniach mobilnych w podobny sposób, jak działa mobilna aplikacja natywna. Serwis www musi posiadać możliwość „zainstalowania” na urządzeniach mobilnych poprzez dodanie ikonki na ekran urządzenia mobilnego, po tej czynności w celu przeglądania treści serwisu, wystarczy kliknąć na ikonkę strony www, a strona będzie działała jak mobilna aplikacja mobilna- treści powinny być częściowo dostępne nawet, bez połączenia z Internetem- technologia Progressive Web Apps (PWA) lub równoważna.
95. Technologia wykonania powinna pozwalać na rozbudowę serwisu www oraz na podłączenie  dodatkowych funkcjonalności w przyszłości.
96. Zarówno serwis www, jak i system CMS powinny być obsługiwane przez najpopularniejsze i najbardziej aktualne przeglądarki: Mozilla Firefox, Google Chrome, Opera, Edge.
97. Wymagane jest zastosowanie technologii PHP, AJAX, PWA bądź innych technologii o porównywalnych możliwościach.
98. Narzędzia do obsługi serwisu www muszą spełniać zalecenia ATAG i być dostępne dla użytkowników niepełnosprawnych, a w szczególności:
	1. Serwis internetowy  powinien dać się obsłużyć przy użyciu klawiatury
	2. Serwis internetowy nie może być zbudowany na bazie tabel, traktowanych jako element konstrukcji layoutu.
	3. Wszystkie elementy graficzne muszą mieć możliwość ustawienia tekstu alternatywnego przez redaktora.
	4. Serwis internetowy powinien oferować dostęp do wszystkich informacji przy wyłączonej obsłudze Java Script.
	5. Wszystkie formularze w serwisie muszą być zgodne ze standardami i przetestowane pod kątem dostępności dla osób niepełnosprawnych.
99. Każdy widok serwisu www musi mieć przez cały czas widoczny link/element graficzny umożliwiający powrót do strony głównej.
100. Zamawiający dopuszcza ze względów bezpieczeństwa danych tylko dedykowane dla jednostek administracji publicznej,  autorskie rozwiązanie CMS, czyli CMS nie może być oparty o rozwiązanie Open Source.

**5. Inne Wymagania dla Wykonawcy.**

W ramach zaoferowanej ceny za wykonanie przedmiotu zamówienia Wykonawca będzie zobowiązany do:

1. wdrożenia wspólnego (tego samego producenta i obsługiwanego w bardzo podobny sposób) systemu CMS dla usługi chmurowej serwisu www, opartych o oddzielne bazy danych, posiadających specyficzne funkcjonalności zgodnie z opisem przedmiotu zamówienia,
2. Przedstawienia zgodnego z wymaganiami projektu graficznego dla serwisu www.
3. Świadczenia usług chmurowych na okres minimum 36 miesięcy, nielimitowanego transferu danych, backupu danych, zabezpieczenia serwera, utrzymania usługi, dostosowywania funkcjonalności strony www do zmieniających się przepisów prawa
4. zapewnienia 50 GB przestrzeni na serwerach dla każdej usługi chmurowej,
5. przeprowadzenia szkolenia online z zakresu obsługi CMS dla usług chmurowych, a także modułów funkcjonalnych, max. po 2 osoby na 1 serwis www,
6. udzielenia gwarancji na przedmiot zamówienia w okresie minimum 36 miesięcy,
7. do usuwania wad i błędów, w tym aktualizacji pod kątem bezpieczeństwa i zgodności z przeglądarkami (m. in. Firefox, Edge, Safari, Opera, Chrome), dokonywania napraw, usuwanie wszelkich usterek funkcjonalnych i technicznych w okresie gwarancji,
8. udzielenia i świadczenia usługi aktualizacji systemu CMS, a także dostosowywania funkcjonalności strony www i elementów technicznych systemu CMS w okresie gwarancji,
9. udzielania bezpłatnych porad telefonicznych (wsparcie techniczne) osobom wskazanym przez Zamawiającego w zakresie obsługi CMS (porady udzielane mają być w dni robocze, tj. od poniedziałku do piątku, w godz. 8.00 - 15.00) przez okres trwania gwarancji,
10. udzielenia niewyłącznej i nieograniczonej terytorialnie licencji na użytkowanie strony www i systemu CMS do jej zarządzania.
11. Przekazania praw autorskich do projektu graficznego strony oraz treści na stronie www.