**Załącznik nr 1 do SWZ – Opis Przedmiotu Zamówienia**

Zamówienie – kompleksowe i całościowe dostarczenie rozwiązania IT w celu polepszenia cyberbezpieczeństwa.

W ramach tego rozwiązania dostarczone zostanie rozwiązanie IT w postaci zarządzalnych urządzeń sieciowych, serwerów fizycznych, zasilania awaryjnego, a także usługi inwentaryzacja, monitorowanie oraz zapewnienie bezpieczeństwa zasobom IT, realizowana przez oprogramowanie do zarządzania i monitorowania infrastruktury IT.

Celem zamówienia jest zwiększenie poziomu cyberbezpieczeństwa ww. podmiotów poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych.  Celem jest wdrożenia mechanizmów i środków zwiększających na ataki z cyberprzestrzeni.

W wyniku podjętych działań przyczyniających się do sprawnego i bezpiecznego działania systemów informatycznych, podniesie się poziom cyberbezpieczeństwa.

W celu wzmocnienia odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych konieczny jest zakup sprzętu, oprogramowania i usług informatycznych w obszarze cyberbezpieczeństwa jako kompleksowego i efektywnego rozwiązania.

Skutkiem realizacji będzie skuteczne zabezpieczenie systemów informatycznych przed cyberprzestępczością w kontekście: ochrony danych osobowych (RODO), potencjalnej utraty danych, ujawnienia wrażliwych danych osobom nieuprawnionym albo umożliwienia atakującym zniszczenia dokumentów lub danych, co zapewni ciągłość pracy oraz zwiększy poczucie bezpieczeństwa.

**Przedmiot obejmuje kompleksowe rozwiązanie, składające się z:**

1. Systemu zabezpieczeń danych;
2. Systemu redundancji danych w chmurze;
3. Zarządzalnych urządzeń sieciowych – 20 szt. switch typ 1, 4 szt. switch typ 2, 3 szt. access point;
4. Serwer fizyczny;
5. Macierz dyskowa;
6. Serwerowe systemy operacyjne;
7. Zasilanie awaryjne – 1 agregat awaryjny, 1 UPS 30 000 VA;
8. System monitorowania serwerów, urządzeń sieciowych, przepływu w sieci 150 szt. ze wsparciem – 1 szt. licencji;
9. System zarządzania zgłoszeniami błędów – 1 szt. licencji;
10. DLP. System zapobiegający wyciekom danych, monitorujący operacje na kluczowych plikach w skład którego wchodzi 90 sztuk licencji do systemu
11. Oprogramowanie wspierające kontrolę – 1 szt. Licencji dla 40 użytkowników;
12. System zarządzania dostępem do sieci 150 szt. na poziomie użytkowników – 1 szt. licencji
13. Oprogramowanie antywirusowe z XDR – 80 szt. licencji na dane oprogramowanie w tym dla 5 serwerów.

Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:

1. Wykonanie Projektu Technicznego dostarczanej infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:

* Dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
* Nazwy oraz szczegółowa adresacja poszczególnych elementów,
* Planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca, zaprojektowanie kompleksowego systemu ochrony danych opartego na funkcjach macierzy oraz oprogramowania standardowego z uwzględnieniem specyfiki całego projektu,
* Wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
* Harmonogram prac.

Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

2. Instalacja oraz konfiguracji oprogramowania zgodnie z wytycznymi Zamawiającego (m.in. wirtualizacja, backup, domena AD)

3. Testy rozwiązania.

4. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.

5. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:

* Specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
* Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
* Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
* Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,
* Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim
* Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury Zamawiającego, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
* Zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni.
* Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

Wymagania w zakresie instalacji i konfiguracji

1. Montaż urządzeń w posiadanej szafie rack 42U w pomieszczeniu udostępnionym przez Zamawiającego.

2. Podłączenie urządzeń do listw zasilających PDU.

3. Aktualizacja oprogramowania układowego wszystkich komponentów.

4. Podłączenie do sieci LAN ( rekonfiguracja przełączników )

5. Wykonawca po zainstalowaniu i skonfigurowaniu sprzętu i oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania dostarczonego sprzętu oraz oprogramowania.

**[SYSTEM ZABEZPIECZEŃ DANYCH]**

1 szt. deduplikator,

|  |  |  |
| --- | --- | --- |
| Lp | Cecha | Opis Wymagań |
|  | Obudowa | Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. |
|  | Kontrolery | Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler. |
|  | Wydajność backupu | Oferowany model deduplikatora musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu co najmniej 5 TB/h (dane podawane przez producenta). Dodatkowo wymagana zagregowana wydajność backupu przy zastosowaniu deduplikacji na źródle co najmniej 15 TB/h (dane podawane przez producenta). |
|  | Wymagana przestrzeń | Przestrzeń użytkowa stworzona w oparciu o dyski NL SAS po zbudowaniu RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności min. 1 dysku musi wynosić min 15 TB. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS o łącznej pojemności RAW min 7 TB jako cache pod zapis backupu. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń *spare* i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji. |
|  | Zabezpieczenia RAID | Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej tolerującej jednoczesną awarię 2 dysków bez utraty danych. |
|  | Rozbudowa | Wymagana możliwość rozbudowy przestrzeni użytkowej poprzez instalację dysków i półek dyskowych oraz dodanie licencji (jeśli będzie wymagana) do min 250 TB. |
|  | Pamięć Cache | Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania. |
|  | Dostępne porty front-end | Urządzenie musi posiadać minimum:  4 porty Ethernet 10 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS, NFS, wszystkie porty wyposażone we wkładki optyczne.  Wymagana możliwość rozbudowy o dodatkowych 8 portów 25G Eth tylko poprzez instalację kart sieciowych. |
|  | Agregacja portów | Wymagana możliwość agregowania portów (bond port). |
|  | Obsługiwane protokoły | Wymagane wsparcie dla FC, NFS, CIFS. |
|  | Zarządzanie | Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak:  - cały deduplikator  - kontrolery  - CPU  - porty front-end  - porty logiczne  - dyski  - file systemy  Pod kątem parametrów takich jak:  - operacje wejścia/wyjścia IOPS  - przepustowość (KB/s lub MB/s)  - czas odpowiedzi (latency)  - średnie użycie (w % dla CPU)  Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych.  Wymagany dostęp do informacji o wykorzystanej fizycznej przestrzeni oraz aktualnym współczynniku redukcji danych.  Wymagane wsparcie dla Multi-factor authentication.  Wymagana możliwość definiowania polityk logowania. |
|  | Redukcja danych | Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.  Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci.  Musi być oficjalne wsparcie producenta dla oferowanego deduplikatora maksymalnego stopnia redukcji danych co najmniej 65:1 |
|  | Kontrola zasobów plikowych | Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni.  Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. |
|  | Ochrona zasobów plikowych | Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system’ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie.  Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM) na poziomie całego file system’u. |
|  | Replikacja danych | Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję.  Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00). |
|  | Wspierane systemy backup | Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam Backup&Replication. |
|  | Licencje | Wymagane jest dostarczenie licencji wieczystych na wszystkie opisane wyżej funkcjonalności. |
|  | Obsługa serwisowa | Deduplikator musi posiadać możliwość upgrade’u firmware-u kontrolerów bez przerywania dostępu do danych.  Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania.  Urządzenie musi umożliwiać zdalne zarządzanie.  Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z legalnego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub partnera serwisowego lub wykonawcę.  Wymagana gwarancja w trybie 9x5 NBD onsite. |

**[SYSTEM REDUNDANCJI W CHMURZE]**

Przedmiotem zamówienia jest rozwiązanie kopii danych w chmurze publicznej jako zabezpieczenie DR na okoliczność incydentów cybernetycznych i fizycznych. Usługa na okres do 30 czerwca 2026.

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| Liczba procesorów | Min. 18 vCPU |
| Pamięć operacyjna | Min. 60GB RAM |
| Przestrzeń dyskowa | Min. 9.6TB SSD |
| Interfejsy sieciowe | Min. 1 szt. 1 Gbit/s |
| Transfer | Min. 30 TB z serwera Nielimitowany do serwer |
| Lokalizacja | W obszarze UE |

.

**[****ZARZĄDZALNE URZĄDZENIA SIECIOWE]**

1. **20 szt. switch typ 1**

Poniżej znajduje się opis dla 1 urządzenia. Zamawiający wymaga dostawy 20 sztuk.

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.

2. Wymagane parametry fizyczne:

2.1 możliwość montażu w stelażu/szafie 19”

2.2 wysokość maksymalna 1U

2.3 głębokość bez zainstalowanego zasilacza nie większa niż 18 cm

2.4 minimum jeden zasilacz 230V AC

2.5 zakres temperatur pracy ciągłej co najmniej od 0°C do +50°C

2.6 zakres wilgotności pracy co najmniej 5% - 90%

2.7 waga bez zainstalowanego zasilacza nie większa niż 2 kg

3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:

3.1 8 portów 100/1000BASE-T

3.2 2 porty 1GE SFP z obsługą modułów 1G-SX, 1G-LX, 1GBase-T (RJ45), kable DAC

3.3 Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.

4. Przełącznik musi posiadać następujące porty służące do zarządzania:

4.1 Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub USB lub port konsoli RS232 ze złączem RJ45

5. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:

5.1 Zarządzanie stosem poprzez jeden adres IP

5.2 Do min. 9 jednostek w stosie

5.3 Porty do stackowania mogą być współdzielone z portami typu uplink.

5.4 Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)

5.5 Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree

5.6 Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.

6. Układ przełączający o wydajności min. 20 Gbps, wydajność przełączania przynajmniej 15 Mpps

7. Obsługa min. 32 000 adresów MAC

8. Wbudowana pamięć RAM min. 2GB. Procesor wielordzeniowy. Minimalne taktowanie procesora 1GHz

9. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1GB

10. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)

11. Możliwość skonfigurowania min. 1024 interfejsów vlan interface SVI działających równocześnie

12. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad

13. Obsługa minimum 120 grup LAG

14. Obsługa ramek jumbo o wielkości min. 9216 bajtów

15. Obsługa sFlow

16. Wsparcie dla G.8032 ERPS

17. Obsługa protokołu VRRP

18. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).

19. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania

20. Obsługa min. 4 000 tras dla routingu IPv4

21. Obsługa min. 1000 tras dla routingu IPv6. Obsługa min. 1024 IPv6 neighbor discovery (ND)

22. Obsługa protokołów związanych z obsługą ruchu typu multicast:

22.1 IGMP Snooping

22.2 MLD Snooping

22.3 minimum 1000 tras multicast

23. Minimalny rozmiar tablicy ARP 4 000 wpisów

24. Obsługa protokołów LLDP i LLDP-MED

25. Przełącznik musi posiadać funkcjonalności dla IPv4 i IPv6: DHCP Server, DHCP Snooping, DHCP relay, DHCP client

26. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

26.1 min. 3 poziomy dostępu administracyjnego poprzez konsolę

26.2 autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL

26.3 możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC

26.4 obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 2048 reguł ACL

26.5 zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 i SSHv2

26.6 możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP

26.7 obsługa mechanizmów Port Security, IP Source Guard, IPv6 RA Guard

26.8 możliwość synchronizacji czasu zgodnie z NTP lub SNTP

27. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:

27.1 klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP

27.2 wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ

28. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).

29. Wymagane opcje zarządzania:

29.1 możliwość lokalnej obserwacji ruchu na określonym porcie

29.2 plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)

29.3 wsparcie dla skryptów python uruchamianych na urządzeniu

29.4 wsparcie dla RMON

30. Wraz z urządzeniami muszą zostać dostarczone:

30.1 pełna dokumentacja w języku polskim lub angielskim

30.2 dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana

31.Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy

32. Urządzenia muszą pochodzić z legalnego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

33. Zamawiający wymaga, aby przełączniki posiadały serwis gwarancyjny świadczony przez producenta lub Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).

W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.

34. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.

System centralnego zarządzania może być dostarczony w formie:

34.1 Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej

Lub

34.2 Dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.

Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.

W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.

System centralnego zarządzania musi umożliwiać:

- tworzenie VLANów

- ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu

- tworzenie połączeń zagregowanych

- monitorowanie statusu pracy przełącznika i portów

- możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania

- możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego

35.Urządzenie musi pochodzić od tego samego producenta co oferowane przełącznik TYP2 w celu zapewnienia spójnego zarządzania siecią.

36.Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.

1. **4 szt. switch typ 2**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.

2. Wymagane parametry fizyczne:

2.1 możliwość montażu w stelażu/szafie 19”

2.2 wysokość maksymalna 1U

2.3 głębokość bez zainstalowanego zasilacza nie większa niż 27 cm

2.4 minimum jeden zasilacz 230V AC

2.5 zakres temperatur pracy ciągłej co najmniej od 0°C do +50°C

2.6 zakres wilgotności pracy co najmniej 5% - 90%

2.7 waga bez zainstalowanego zasilacza nie większa niż 3 kg

3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:

3.1 24 porty 100/1000BASE-T PoE+ zgodnych ze standardem 802.3at (minimalny budżet mocy PoE: 370W)

3.2 4 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T, kabli DAC

3.3 Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.

4. Przełącznik musi posiadać następujące porty służące do zarządzania:

4.1 Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub USB lub port konsoli RS232 ze złączem RJ45

5. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:

5.1 Zarządzanie stosem poprzez jeden adres IP

5.2 Do min. 9 jednostek w stosie

5.3 Porty do stackowania mogą być współdzielone z portami typu uplink.

5.4 Magistrala stackująca o wydajności minimum 80Gb/s

5.5 Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)

5.6 Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree

5.7 Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.

6.Układ przełączający o wydajności min. 176 Gbps, wydajność przełączania przynajmniej 132 Mpps

7. Obsługa min. 32 000 adresów MAC

8. Wbudowana pamięć RAM min. 2GB. Procesor wielordzeniowy. Minimalne taktowanie procesora 1GHz

9. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1GB

10. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)

11. Możliwość skonfigurowania min. 1024 interfejsów vlan interface SVI działających równocześnie

12. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad

13. Obsługa minimum 120 grup LAG

14. Obsługa ramek jumbo o wielkości min. 9216 bajtów

15. Obsługa sFlow

16. Wsparcie dla G.8032 ERPS

17. Obsługa protokołu VRRP

18. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).

19. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania

20. Obsługa min. 4 000 tras dla routingu IPv4

21 Obsługa min. 1000 tras dla routingu IPv6

21.1 Obsługa min. 1024 IPv6 neighbor discovery (ND)

22. Obsługa protokołów związanych z obsługą ruchu typu multicast:

22.1 IGMP Snooping

22.2 MLD Snooping

22.3 minimum 1000 tras multicast

23. Minimalny rozmiar tablicy ARP 4 000 wpisów

24. Obsługa protokołów LLDP i LLDP-MED

25. Przełącznik musi posiadać funkcjonalności dla IPv4 i IPv6: DHCP Server, DHCP Snooping, DHCP relay, DHCP client

26. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

26.1 min. 3 poziomy dostępu administracyjnego poprzez konsolę

26.2 autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL

26.3 możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC

26.4 obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 500 reguł ACL

26.5 zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 i SSHv2

26.6 możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP

26.7 obsługa mechanizmów Port Security, IP Source Guard, IPv6 RA Guard

26.8 możliwość synchronizacji czasu zgodnie z NTP lub SNTP

27. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:

27.1 klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP

27.2 wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ

28. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).

29. Wymagane opcje zarządzania:

29.1 możliwość lokalnej obserwacji ruchu na określonym porcie

29.2 plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)

29.3 wsparcie dla skyptów python uruchamianych na urządzeniu

29.4 wsparcie dla RMON

30. Wraz z urządzeniami muszą zostać dostarczone:

30.1 pełna dokumentacja w języku polskim lub angielskim

30.2 dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana

31. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy

32. Urządzenia muszą pochodzić z legalnego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

33. Zamawiający wymaga, aby przełączniki posiadały serwis gwarancyjny świadczony przez producenta lub Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).

W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.

34. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.

System centralnego zarządzania może być dostarczony w formie:

34.1 Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej

Lub

34.2 Dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.

Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.

W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.

System centralnego zarządzania musi umożliwiać:

- tworzenie VLANów

- ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu

- tworzenie połączeń zagregowanych

- monitorowanie statusu pracy przełącznika i portów

- możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania

- możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego

35.Urządzenie musi pochodzić od tego samego producenta co oferowane przełącznik TYP1 w celu zapewnienia spójnego zarządzania siecią.

36. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.

1. **3 szt. access point**

1. Punkt dostępowy musi być dedykowanym urządzeniem sieciowym przystosowanym do zamontowania na suficie i na ścianie. Wymagane dostarczenie z zestawu montażowego. System operacyjny (firmware) musi być dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej. Oprogramowanie do pracy w trybie tzw „lekkiego AP”, możliwość pracy jako tzw “grubego AP (FAT AP)” oraz możliwość pracy jako tzw. Kontroler AP, czyli jeden z punktów dostępowych musi mieć możliwość pracy jako kontroler WLAN.

2. Urządzenie w trybie FAT musi umożliwiać zarządzać pracą dodatkowych access-pointów tego samego producenta. Funkcjonalność zarządzania pracą pozostałymi access-pointami musi umożliwiać transfer ruchu w trybie „local forwarding” (ruch z każdego access-pointa przesyłany jest w bezpośrednio w sieci lokalnej) oraz „Gateway” (access-point w trybie FAT działa jako brama sieci dla pozostałych access-pointów, realizując m.in. funkcjonalność NAT). Funkcjonalność zarządzania pracą pozostałymi urządzeniami musi być realizowana z poziomu przeglądarki urządzenia FAT, jak również z poziomu CLI (z wykorzystaniem m.in. protokołu SSH) urządzenia FAT

3. Wymagane parametry fizyczne:

3.1 możliwość montażu na suficie oraz ścianie (wraz z urządzeniem należy dostarczyć elementy to montowania)

3.2 wysokość maksymalna 51 mm

3.3 możliwość zasilania przez zasilacz DC

3.4 zakres temperatur pracy ciągłej co najmniej -10°C – +50°C

3.5 zakres wilgotności pracy co najmniej 5% - 90%

3.6 waga nie większa niż 1,09kg

3.7 Pyłoszczelność i wodoodporność na poziomie IP41

4. Punkt dostępowy musi posiadać:

4.1 dedykowany port konsolowy fizyczny lub bluetooth

4.2 minimum 1 porty 100/1000Mbit Base-T PoE

4.3 minimum 1 port USB

5. Obsługiwane standardy radiowe: 802.11a/b/g/n/ac/ac Wave 2/11ax, jednoczesna obsługa minimum 16 SSID dla każdego radia

6. Wbudowane anteny minimum 4dBi dla 2,4GHz oraz 5dBi dla 5GHz z pracą w standardzie minimum MIMO: 2.4G: 2x2, 5G: 2x2

7. Wsparcie dla standardów/funkcjonalności bezpieczeństwa: WPA, WPA2, WPA3, 802.1x, IP Source Guard (IPSG) oraz tworzenie ACL

8. Wsparcie dla roamingu zgodnego z 802.11k, 802.11v, 802.11r

9. Obsługa minimum 1000 równocześnie podłączonych użytkowników do punktu dostępowego

10. Wydajność minimum 1,7Gbps w tym minimum 500Mbps dla 2.4GHz oraz 1,2Gbps dla 5GHz

11. Obsługa BLE w wersji 5.2

12. Zużycie mocy nie większe niż 13W

13. Możliwość zarządzania poprzez:

13.1 WWW over HTTPS

13.2 kontroler tego samego producenta

13.3 SNMP v1, v2c, v3,

13.4 Dedykowany port konsoli

13.5 SSHv2

14. Kompatybilność dla protokołów oraz standardów sieciowych takich jak: IPv6, LLDP, mDNS, NAT, IPsec

16. Tunel CAPWAP dla komunikacji z kontrolerem muszą być zaszyfrowane celem ochrony przed możliwością podsłuchania transmisji w sieci kablowej

17. Wsparcie dla protokołów i standardów:

17.1 802.11e

17.2 802.11i

17.3 802.11d

17.4 802.11h

17.5 802.11u

17.6 802.11w

17.7 802.15.1

17.8 LLDP

17.10 DTLS encryption

17.11 A-MPDU i A-MSDU

18. Obsługa NTP lub SNTP

19. Wraz z urządzeniami muszą zostać dostarczone:

19.1 pełna dokumentacja w języku polskim lub angielskim

19.2 dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana

20. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

21. Urządzenia muszą pochodzić z legalnego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski

22. Zamawiający wymaga, aby urządzenia posiadały serwis gwarancyjny świadczony przez producenta lub Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).

W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.

23.Wraz z urządzeniem należy dostarczyć system centralnego zarządzania pochodzący od producenta oferowanych urządzeń.

System centralnego zarządzania może być dostarczony w formie:

23.1. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej

Lub

23.2. Dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.

Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.

W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.

System centralnego zarządzania musi umożliwiać:

- tworzenie VLANów

- tworzenie SSID dla sieci WiFi z możliwością przypisania VLANu

- tworzenie zabezpieczeń dla SSID

- monitorowanie statusu pracy punktów dostępowych

- możliwość uruchomienia CLI w panelu systemu do zarządzania

- możliwość wykonania aktualizacji oprogramowania dla danego punktu dostępowego

24. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.

**[SERWER FIZYCZNY]**

Minimalne wymaganie dotyczące serwera:

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| Obudowa | Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do mocowania kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia)  Serwer wyposażony w zdejmowany panel przedni z zamkiem chroniącym przed nieuprawionym dostępem do dysków oraz możliwością dołożenia czujnika otwarcia obudowy współpracującego z BIOS/UEFI. |
| Procesor | Dwa procesory dwunastordzeniowe, x86 - 64 bity, pracujące z częstotliwością bazową min. 2.0GHz i osiągające w testach SPECrate2017\_int\_base wynik nie gorszy niż 216 punktów, dla testu oferowanego modelu serwera z 2 procesorami.  W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie [www.spec.org](about:blank)  Płyta główna wspierająca zastosowanie procesorów od 8 do 60 rdzeni, mocy do min. 350W i taktowaniu CPU do min. 3.7GHz. |
| Liczba procesorów | Min. 2 procesory |
| Pamięć operacyjna | Min. 512GB RDIMM DDR5 4800 MT/s w modułach pamięci o pojemności min. 32 GB każdy  Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB. |
| Sloty rozszerzeń | Min. 3 aktywnych gniazd PCI-Express generacji 5, x16 (szybkość slotu – bus width). 1x gniazda pełnej wysokości (full height) 2x gniazda połówkowej wysokości gotowe do obsadzenia kartami z portami zewnętrznymi.  Dwa sloty OCP 3.0 możliwe do obsadzenia poprzez kontrolery sprzętowe dla dysków lub karty sieciowe w dowolnej konfiguracji. |
| Dysk twardy | Serwer bez klatkowy z możliwością rozbudowy/rekonfiguracji w przyszłości serwera do 10 dysków typu Hot Swap, SAS/SATA/SSD/NVMe, 2,5” montowane z przodu obudowy.  W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 10 zatoki dyskowe SFF gotowe do instalacji dysków SAS/SATA/SSD/NVMe 2,5”typu Hot Swap.  Zainstalowane min. 2szt. dysków SSD NVMe 960GB nie zajmujące wnęk na dyski twarde pracujące w konfiguracji ze sprzętowym  RAID 1. |
| Kontroler | Serwer wyposażony w kontroler software dla dysków SATA, obsługujący poziomy: RAID 0, 1, 5, 10.  Możliwość zastosowania/wymiany kontrolera na kontroler sprzętowy wyposażony w min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SSD/SATA/SAS/NVMe.  Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie. |
| Interfejsy sieciowe | Jedna dwuportowa karta 10Gb Base-T oparta o chipset BMC57416. |
| Karta graficzna | Zintegrowana karta graficzna |
| Porty | 5 x USB, z czego min 4szt w wersji USB 3.2 oraz jeden port USB 2.0  1x VGA  Możliwość rozbudowy/rekonfiguracji o:  - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express  - cyfrowy port video ( Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USB 8 |
| Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W. |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |
| Diagnostyka | Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze. |
| Bezpieczeństwo | Serwer wyposażony w moduł TPM 2.0. |
| Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:   * monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe * praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP * dostęp do karty zarządzającej poprzez   + dedykowany port RJ45 z tyłu serwera lub   + przez współdzielony port zintegrowanej karty sieciowej serwera   dostęp do karty możliwy   * + z poziomu przeglądarki webowej (GUI)   + z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)   + z poziomu skryptu (XML/Perl)   + poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) * 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 przekierowanie SNMP (SNMP passthrough) * uwierzytelnianie oprogramowania sprzętowego PCIe z protokołem bezpieczeństwa i modelem danych (SPDM) zapewnia integralność komponentu * obsługa zdalnego serwera logowania (remote syslog) * wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów * mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie * funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności * 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) * zarządzanie grupami serwerów, w tym:   + tworzenie i konfiguracja grup serwerów   + sterowanie zasilaniem (wł/wył)   + ograniczenie poboru mocy dla grupy (power capping)   + aktualizacja oprogramowania (firmware)   + wspólne wirtualne media dla grupy * możliwość równoczesnej obsługi przez 6 administratorów * autentykacja dwuskładnikowa (Kerberos) * wsparcie dla Microsoft Active Directory * obsługa SSL i SSH * enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli * wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API * wsparcie dla Integrated Remote Console for Windows clients * możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) |
| Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Serwer jest dostarczany bez Systemu operacyjnego  Zapewnia wsparcie dla:  Microsoft Windows Server 2019, 2022  Ubuntu 22.04 LTS  Red Hat Enterprise Linux (RHEL) 8.6 oraz 9.0  SUSE Linux Enterprise Server (SLES) 15 SP4  VMware ESXi 7.0 U3, 8.0 |
| Wsparcie techniczne | Gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z 4-godzinnym czasem reakcji przez całą dobę (przybycie na miejsce). 15-minutowy czas reakcji na zdarzenia krytyczne przez całą dobę, 7 dni w tygodniu.  Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń lub wykonawcę. |
| Inne | Urządzenia muszą być zakupione w legalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z legalnego kanału dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub równoważnymi.  Deklaracja zgodności CE. |

INORMACJA

Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie przedmiotu zamówienia, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego.

Zamieszczone w specyfikacji nazwy technologicznych lub producentów kluczowych komponentów użyto jedynie w celu przykładowym.

Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w opisie przedmiotu zamówienia mogą być zastąpione urządzeniami bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie przedmiotu zamówienia. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w niniejszym zaproszeniu, ani do zmiany ceny.

**[MACIERZ DYSKOWA]**

1x NAS

Minimalne wymagania:

|  |  |
| --- | --- |
| Procesor | Procesor wielordzeniowy osiągający w teście PassMark minimum 3900 punktów. |
| Obudowa | Typu RACK o wysokości maksymalnie 2U wraz z kompatybilnymi szynami przesuwnymi do montażu w szafie rack w zestawie. |
| Pamięć RAM | Minimum 8 GB DDR4. |
| Ilość obsługiwanych dysków | 8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s o pojemności maksymalnej dysku min. 22TB |
| Zainstalowane dyski | 8 dysków o pojemności 8TB każdy zgodnch z listą kompatybilności oferowanego serwera oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - pamięć cache: minimum 256MB, - gwarancja: minimum 36 miesięcy, - MTBF: minimum 1 milion, - usługa odzyskiwania danych. |
| Interfejsy sieciowe | Minimum 2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M) |
| * obsługa VLAN i Jumbo Frame, * Możliwość zamontowania dodatkowej karty z interfejsami 10Gb (SFP+), * Możliwość zamontowania dodatkowej karty z interfejsami 25Gb (SFP28), |
| Porty | 2x USB 2.0, 2x USB 3.2 Gen 2, 1x HDMI 1.4b |
| Wskaźniki LED | HDD 1–8, stan, LAN, rozszerzenie, zasilanie |
| Obsługa RAID | Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk. |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Szyfrowanie | Możliwość szyfrowania całych woluminów kluczem AES 256 bitów. |
| System Operacyjny | Apple Mac OS 10.10 lub nowszy.  Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux.  IBM AIX 7, Solaris 10 lub nowszy.  Microsoft Windows 7, 8, 10, 11  Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019. |
| Stacja monitoringu | Minimum 8 licencji na podłączenie kamer w aplikacji do monitoringu. |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, możliwość tworzenia maszyn wirtualnych bezpośrednio na serwerze NAS bez zewnętrznego wirtualizatora, Obsługa automatycznego warstwowania danych tzw. auto tiering. |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów |
| Język GUI | Polski |
| Gwarancja | Gwarancji producenta. |
| Waga urządzenia  (bez dysków) | Maksymalnie 12 kg |
| Pobór mocy | Maksymalnie 60W w trybie pracy. |
| System plików | Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| Liczba kont użytkowników | Minimum 4090 |
| Liczba grup | Minimum 500 |
| Liczba udziałów | Minimum 500 |
| Ilość połączń z maksymalną pamięcią RAM (CIFS) | Minimum 1500 |
| Maksymalna liczba migawek | Minimum 1000 |
| Zasilanie | Redundantny zasilacz o mocy minimum 250W (100-240V) |
| Wentylatory | Minimum 2 wentylatory o rozmiarze 40mm, 12VDC |
| UPS | Obsługa sieciowych awaryjnych zasilaczy UPS. |

**[SERWEROWE SYSTEMY OPERACYJNE]**

**Zamawiający oczekuje dostawy dwóch systemów.**

**Minimalne wymaganie dotyczące pierwszego, wymaganego systemu:**

|  |  |
| --- | --- |
| **LP.** | **Wymagania funkcjonalno-techniczne (minimalne)** |
| 1 | Licencja na oprogramowanie musi pozwalać na pełne wykorzystanie sprzętowych zasobów serwera |
| 2 | Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych |
| 3 | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. |
| 4 | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 320 logicznych wątków oraz do 4TB pamięci fizycznej RAM. |
| 5 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-64 procesorowych. |
| 6 | Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB |
| 7 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM. |
| 8 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych. |
| 9 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć co najmniej 4 porty szeregowe i 3 porty równoległe i 20 urządzeń USB. |
| 10 | Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. |
| 11 | Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. |
| 12 | Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade).  Licencjonowanie nie może odbywać się w trybie OEM. |
| 13 | Rozwiązanie musi umożliwiać poprawne zainstalowanie następujących systemów operacyjnych: Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11, SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris 11,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 12.04, SCO OpenServer, SCO Unixware, Mac OS X |
| 14 | Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. |
| 15 | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. |
| 16 | Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. |
| 17 | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.  Z możliwością wysyłania maila o wykonanej kopii bezpieczeństwa |
| 18 | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. |
| 19 | Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. |
| 20 | Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. |
| 21 | Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. |
| 22 | Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. |
| 23 | System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. |
| 24 | Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. |
| 25 | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). |
| 26 | Należy dostarczyć licencję obsługującą 3 serwery po 2 procesory. |

**Minimalne wymaganie dotyczące drugiego, wymaganego systemu:**

Przedmiotem zamówienia jest zakup nowej licencji Microsoft SQL Server Standard Perpetual lub licencji równoważnej.

Wymagania ogólne:

1. Licencje muszą być dostarczone w formie elektronicznej. Stan licencji musi być widoczny na indywidualnym profilu Zamawiającego w portalu producenta oprogramowania przeznaczonym do zarządzania licencjami oprogramowania producenta.

2. Oferowane licencje muszą być nowe, zakupione w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

Minimalne wymagania dla licencji równoważnej:

1. W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska.

2. W przypadku zaoferowania przez Wykonawcę licencji równoważnych Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane licencje.

3. W przypadku, gdy zaoferowane przez Wykonawcę licencje równoważne nie będą właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu licencji równoważnych oraz dostarczy inne rozwiązania spełniające wymagania SOPZ.

4. Licencje równoważne dostarczane przez Wykonawcę nie mogą powodować utraty kompatybilności oraz wsparcia/gwarancji producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.

5. Licencje równoważne zastosowane przez Wykonawcę nie mogą w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie licencji równoważnych, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie licencji równoważnych, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

6. Zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.

7. W przypadku dostarczania licencji, równoważnych względem wyspecyfikowanej przez Zamawiającego w Szczegółowym Opisie Przedmiotu Zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczone licencje spełniają wszystkie wymagania i warunki określone w Szczegółowym Opisie Przedmiotu Zamówienia.

Zamawiający wymaga także dostawy wraz z powyższym oprogramowaniem licencje dostępowe do powyżej opisanego systemu operacyjnego Microsoft SQL Server Standard Perpetual lub równoważny w ilości 30 szt. Oferowane licencje muszą udostępnić możliwość korzystania z zasobów serwisów 30 użytkownikom.

**[****ZASILANIE AWARYJNE]**

1. **1 x agregat awaryjny**

Minimalne wymaganie dotyczące jednej sztuki agregatu:

Agregat prądotwórczy ma być wykonany w obudowie zewnętrznej wyciszonej w obudowie pokryta proszkowo farbą epoksydową.

Agregat powinien być wyposażony w nowoczesny panel kontroli ze sterowaniem mikroprocesorowym z możliwością programowania podstawowych parametrów pracy.

Panel sterowania powinien być zabezpieczony zamykanymi drzwiami z przeszklonym wizjerem.

Agregat ma być wyposażony w nowoczesny silnik wysokoprężny zapewniający dobrą stabilizację częstotliwości i diagnostykę oraz w główne zabezpieczenie – wyłącznik kompaktowy.

W ramach dostawy zawarte mają być:

1. dostawa agregatu w obudowie zewnętrznej o podanych parametrach na miejsce instalacji
2. dostawa SZR na przełączniku do agregatu
3. przeszkolenie obsługi pod względem prawidłowej eksploatacji
4. dokumentacja w języku polskim
5. test prawidłowego działania systemu pod sztucznym obciążeniem w celu sprawdzenia poprawności działania.
6. pełna dokumentacja agregatu wraz z zalaminowaną stanowiskową, skróconą instrukcją obsługi

Oferowane urządzenia (dotyczy silnika i prądnicy oraz całego agregatu) są fabrycznie nowe, bez śladu użytkowania i posiadają stosowny pakiet usług gwarancyjnych, pochodzą z legalnego kanału sprzedaży, posiadają serwis i wparcie producenta.

**Główne parametry agregatu .**

Częstotliwość Hz 50

Napięcie V 400

Współczynnik mocy cos ϕ 0.8

Liczba faz 3 Moc Moc maksymalna

LTP kVA 64,82 Moc maksymalna

PRP kW 46.49 Moc znamionowa

PRP kVA 58,11 Moc znamionowa

LTP kW 51.85 Moc maksymalna

Zoptymalizowana emisja spalin wg 97/68 50Hz (COM) Non Emission Certified

System chłodzenia silnika Woda

Liczba cylindrów i układ 4 w rzędzie

Pojemność cm³ 4040

Zasilanie Turbodoładowany z intercoolerem

Regulator obrotów Elektroniczny

Moc znamionowa PRP SILNIKA 60

Pojemność układu smarowania l 8.5

Paliwo Diesel

Szczególne zużycie paliwa przy 75% PRP g/kWh 214

Szczególne zużycie paliwa @ PRP g/kWh

System rozruchu Elektryczny

Napięcie instalacji V 12

Pojemność zbiornika paliwa l 125

Praca przy obciazeniu 75% - 12 h

**Prądnica**

Napięcie V 400

Częstotliwość Hz 50

Współczynnik mocy cos ϕ 0.8

Typ Bezszczotkowy

Bieguny 4

Standardowy AVR - DSR DIGITAL

Tolerancja napięcia % 1

Sprawność @ 100% obciążenia % 90,7

Klasa izolacji H

Klasa IP 23

**Budowa**

Konstrukcja, która zapewnia łatwy dostęp do połączeń oraz części podczas przeglądów okresowych.

**Regulator napięcia**

Za kontrolę generowanego napięcia odpowiedzialny jest cyfrowy regulator DSR. Stabilność napięcia wynosi ±1% w stanie ustalonym niezależnie od współczynnika mocy oraz zmiany obrotów w zakresie od -5% do +30% obrotów znamionowych.

**Uzwojenia / System wzbudzenia**

Stojan alternatora jest nawinięty z poskokiem 2/3. Zapewnia to eliminację krotności trzeciej harmonicznej (3, 9, 15, itd.) napięcia wyjściowego. Uznawane jest to za najlepsze rozwiązanie w celu niezawodnego zasilania odbiorników nieliniowych. Poskok 2/3 minimalizuje indukowanie się nadmiernych prądów w obwodzie neutralnym. MAUX - Uzwojenie Dodatkowe MeccAlte jest oddzielnym uzwojeniem w stojanie zasilającym regulator napięcia. Uzwojenie to umożliwia przejęcie 300% obciążenia znamionowego przez 20 sekund. Umożliwia to niezawodny rozruch silników elektrycznych. Izolacja / Impregnacja Izolacja jest klasy H. Uzwojenia zostały zaimpregnowane najwyższej jakości żywicą epoksydową Normy wykonania Alternator został wykonany zgodnie z najbardziej powszechnymi normami, tj. CEI 2-3, IEC 34-1, EN lub równoważnymi.

**Normy wykonania**

Alternator został wykonany zgodnie z najbardziej powszechnymi normami, tj. CEI 2-3, IEC 34-1, EN 60034-1, VDE 0530, BS 4999-5000, CAN/CSA-C22.2 No14-95- No100-95 lub równoważne.

**Wyposażenie agregatu**

**PODSTAWA WYKONANA ZE SPAWANYCH STALOWYCH PROFILI, WYPOSAŻONA W:**

• Amortyzatory drgań o odpowiedniej wielkości

• Spawane nogi podporowe

**PLASTIKOWY ZBIORNIK PALIWA WYPOSAŻONY W:**

• Wlew • Odmę (wentylację)

• Czujnik poziomu paliwa

Nie dopuszcza się metalowych zbiorników paliwa.

**RURKA SPUSTOWA OLEJU:**

**•** Ułatwiony spust oleju

**OBUDOWA:**

• Wyciszona obudowa wykonana z modułowych ocynkowanych stalowych paneli w celu ochrony przed korozją oraz agresywnymi warunkami.

• Łatwy dostęp w celu okresowej obsługi.

• Zamykane drzwi zabezpieczające panel sterowania z oknem

• Boczna czerpnia powietrza odpowiednio zabezpieczona i wyciszona. Górna zabezpieczona wyrzutnia powietrza.

• Pojedynczy centralny uchwyt transportowy na dachu z możliwością odłączenia.

**WYCISZENIE:**

• Obudowa wyciszona

• Wydajny tłumik umieszczony wewnątrz obudowy

Zużycie paliwa @ 75% PRP l/h 10.30

Zużycie paliwa @ 100% PRP l/h 13.89

Czas pracy przy @ 75% PRP h 12.14

Czas pracy przy @ 100% PRP h 9

Poziom ciśnienia akustycznego z 7 m dB(A) 63

Automatyczny Panel

Sterowania Automatyczny panel sterowania na agregacie, wyposażony w cyfrowy sterownik dla monitorowania, sterowania i zabezpieczenia agregatu, zabezpieczony zamykanymi drzwiami.

• Napięcie agregatu (3 fazy).

• Napięcie sieci.

• Częstotliwość agregatu.

• Prąd agregatu (3 fazy).

• Napięcie akumulatora.

• Moc (kVA - kW - kVAr).

• Współczynnik mocy Cos φ.

• Licznik motogodzin.

• Obroty silnika r.p.m.

• Poziom paliwa (%).

**STEROWANIE I INNE**

• Cztery tryby pracy: OFF - Ręczny start - Automatyczny start - Automatyczny test

• Przyciski wymuszenia zasilania z agregatu lub z sieci

• Przyciski: start/stop, reset błędu, góra/dół/strona/wybór

• Wyłącznik awaryjny agregatu

• Możliwość zdalnego startu.

• Alarm dźwiękowy

• Port komunikacyjny wbudowany w panel sterowania agregatem

• Wyłącznik zasilania DC

• Automatyczny prostownik akumulatora

• Możliwość ustawienia HASŁA bezpieczeństwa

SZR do agregatu na przełączniku posiadający blokadę mechaniczną i elektryczną z wyłącznikiem awaryjnym zamontowanym na obudowie SZR

**ZABEZPIECZENIA Z ALARMEM**

• Zabezpieczenia silnika: niski poziom paliwa, niskie ciśnienie oleju, wysoka temperatura sinika

• Zabezpieczenia agregatu: niskie/wysokie napięcie, przeciążenie, niska/wysoka częstotliwość, nieudany rozruch, niskie/wysokie napięcie akumulatora, awaria prostownika akumulatora

**ZABEZPIECZENIA Z WYŁĄCZENIEM**

• Zabezpieczenia silnika: niski poziom paliwa, niskie ciśnienie oleju, wysoka temperatura sinika

• Zabezpieczenia agregatu: niskie/wysokie napięcie, przeciążenie, niskie/wysokie napięcie akumulatora

• Wyłącznik: III-biegunowy • Przekroczony prąd doziemny .

**INNE ZABEZPIECZENIA**

• Wyłącznik awaryjny.

• Panel zabezpieczony zamykanymi drzwiami

1. **1 x UPS 30 000 VA**

Minimalne wymagania dla zasilacza UPS:

|  |  |  |
| --- | --- | --- |
| Moc | | 30 kVA |
| 30 kW |
| Klasyfikacja (PN-EN IEC 62040-3) | | On-Line, podwójna konwersja, VFI SS 111 |
| Normy | | PN-EN IEC 62040-1 |
| PN-EN IEC 62040-2 |
| PN-EN IEC 62040-3  Lub równoważne |
| Typ zabudowy | | Tower |
| Wejście - zasilanie | Liczba faz | 3 |
| Napięcie znamionowe | 380 / 400 / 415 V |
| Zakres napięcia | 201 ÷ 478 V |
| Częstotliwość znamionowa | 50 / 60 Hz (autodetekcja) |
| Zakres częstotliwości | 40 ÷ 72 Hz |
| Współczynnik mocy (PF) | ≥ 0,99 |
| Zniekształcenia harmoniczne (THDi) | ≤ 3 % |
|  |
| Zgodność z systemem zasilania | TN-S / TN-C / TN-C-S / TT |  |
| Sposób podłączenia | 3P + N + PE (listwa zaciskowa) |  |
| Wejście - tor obejścia (bypass) | Liczba faz | 3 |  |
| Napięcie znamionowe | 380 / 400 / 415 V |  |
| Zakres napięcia | 338 ÷ 458 V |  |
| Częstotliwość znamionowa | 50 / 60 Hz |  |
| Sposób podłączenia | 3P + N + PE (listwa zaciskowa) |  |
| Akumulatory | Technologia akumulatorów | VRLA / AGM / NiCd / Li |  |
| Napięcie nominalne łańcucha akumulatorów | ± 480 V DC |  |
| Opcjonalne napięcie łańcucha akumulatorów | 320 ÷ 607 V DC |  |
| Napięcie nominalne pojedynczego akumulatoróa | 12 V DC |  |
| Ilość akumulatorów nominalna | 40 szt. |  |
| Pojemność obsługiwanych akumulatorów wewnętrznych | 7 Ah / 9 Ah / 10 Ah |  |
| Możliwość podłączenia akumulatorów zewnętrznych | tak |  |
| Montaż akumulatorów | wewnątrz zasilacza |  |
| dedykowane obudowy EBM dostosowane do akumulatorów 7 / 9 / 10 Ah |  |
| otwarte stojaki STB dla akumulatorów  o większych pojemnościach |  |
| Prąd ładowania nominalny | 30 A |  |
| Czas ładowania wewnętrznych akumulatorów | zależny od zastosowanych akumulatorów |  |
| Sposób podłączenia akumulatorów | + / PE / - (listwa zaciskowa) |  |
| Wyjście | Liczba faz | 3 |  |
| Napięcie wyjściowe | 380 / 400 / 415 V (konfigurowalne) |  |
| Tolerancja napięcia w trybie pracy z sieci | ± 1 % dla obciążenia zrównoważonego  ± 2 % dla obciążenia niezrównoważonego |  |
| Częstotliwość przy pracy z sieci | synchronizowana |  |
| Częstotliwość przy pracy z akumulatorów | 50 / 60 Hz |  |
| Dokładność częstotliwości przy pracy z akumulatorów | ± 0,1 % |  |
| Przebieg napięcia | fala sinusoidalna |  |
| Współczynnik mocy (PF) | 1 |  |
| Współczynnik szczytu (CF) | 3:1 |  |
| Zniekształcenia harmoniczne (THDu) | ≤ 2 % (obciążenie liniowe) |  |
| ≤ 5 % (obciążenie nieliniowe) |  |
| Zdolność przeciążeniowa | 102 ÷ 110 % do 60 min |  |
| 110 ÷ 125 % do 10 min |  |
| 125 ÷ 150 % do 1 min |  |
| > 150 % do 150 ms |  |
| Sposób podłączenia | 3P + N + PE (listwa zaciskowa) |  |
| System | Sprawność w trybie sieci | ≥ 95,8 % |  |
| Sprawność w trybie ECO | ≥ 99 % |  |
| Czas przełączenia | 0 ms |  |
| Funkcje rozruchu | Zimny start (COLD START) Miękki start (SOFT START) |  |
| Interfejs użytkownika | wyświetlacz dotykowy LCD 5" |  |
| Interfejs użytkownika -dostępne języki | 10 |  |
| Obsługa w języku polskim | tak |  |
| Złącze EPO | tak |  |
| Zabezpieczenia | zwarciowe |  |
| przeciążeniowe |  |
| temperaturowe |  |
| Filtr przeciwzakłóceniowy | RFI |  |
| EMI |  |
| Alarmy | przeciążenie |  |
| praca z akumulatorów |  |
| niskie napięcie akumulatorów |  |
| awaria wentylatorów |  |
| Praca równoległa | do 4 jednostek |  |
| EMI | PN-EN IEC 62040-2 |  |
| EMS | PN-EN 61000-4-2 |  |
| PN-EN IEC 61000-4-3 |  |
| PN-EN 61000-4-4 |  |
| PN-EN 61000-4-5  Lub równoważne |  |
| Komunikacja | Interfejsy | USB (typ B) |  |
| RS232 |  |
| styki bezpotencjałowe |  |
| 2 x złącze kart rozszerzeń |  |
| Obsługa systemów operacyjnych | MS Windows / Linux / Unix / MacOS |  |
| Cechy | Wymiary (szer. x wys. x gł.) | 500 x 860 x 887 mm |  |
| Waga bez akumulatorów | 45 kg |  |
| Kolor obudowy | czarny |  |
| Temperatura pracy | 0 °C ÷ 40 °C |  |
| Wilgotność | 5 ÷ 95 % (bez kondensacji) |  |
| Głośność (@ 1 m) | ≤ 65 dB |  |
| Stopień ochrony (PN-EN 60529:2003) | IP 20 |  |
| Montaż zasilacza | pionowy, wolnostojący |  |
| Wysokość robocza bez obniżenia mocy | 0 ÷ 1500 m n.p.m. |  |
| Wysokość robocza z obniżeniem mocy | obniżenie mocy o 1 % co 100 m |  |
| w zakresie 1500 ÷ 2000 m n.p.m. |  |

**[SYSTEM MONITOROWANIA SERWERÓW, URZĄDZEŃ SIECIOWYCH, PRZEPŁYWU W SIECI 150 szt. ZE WSPARCIEM]**

1 szt. licencji na system monitorowania

Zamawiający wykorzystuje oprogramowanie Event Sentry Log Monitoring. Należy dostarczyć jedną licencję systemu lub system równoważny.

1. Monitorowanie logów

- Równoważny system musi zapewniać kompleksowe monitorowanie logów z różnych źródeł, w tym serwerów, urządzeń sieciowych, aplikacji oraz systemów operacyjnych.

- System powinien zbierać, analizować i przechowywać logi w czasie rzeczywistym, umożliwiając natychmiastową reakcję na potencjalne incydenty.

- Obsługa standardowych protokołów, takich jak Syslog, SNMP, Windows Event Log oraz innych źródeł logów, musi być zagwarantowana.

2. Analiza i korelacja zdarzeń

- Równoważny system powinien oferować możliwość zaawansowanej analizy oraz korelacji zdarzeń w celu wykrycia wzorców, które mogą wskazywać na zagrożenia, anomalie lub problemy w infrastrukturze IT.

- System powinien obsługiwać tworzenie reguł korelacyjnych, które pozwalają na identyfikację złożonych zagrożeń lub nietypowych działań na podstawie różnych zdarzeń rejestrowanych w logach.

3. Alertowanie i powiadamianie

- System musi zapewniać natychmiastowe powiadomienia o krytycznych zdarzeniach wykrytych w logach, wysyłając alerty przez e-mail, SMS lub inne kanały.

- Powiadomienia powinny być dostosowywane do różnych poziomów krytyczności oraz rodzaju incydentu, z możliwością definiowania różnych warunków i progów dla generowania alertów.

4. Raportowanie i audyt

- System równoważny musi oferować rozbudowane funkcje raportowania, pozwalające na generowanie raportów na temat monitorowanych zdarzeń, zgodności z regulacjami, wydajności systemów oraz wykrytych zagrożeń.

- Raporty muszą być dostępne w formatach graficznych i tekstowych (PDF, CSV, Excel), z możliwością automatycznego generowania ich na podstawie zaplanowanego harmonogramu.

- System powinien umożliwiać audyt zdarzeń zgodny z wymaganiami branżowymi, takimi jak RODO, PCI DSS, czy ISO 27001.

5. Zarządzanie logami

- Równoważny system musi zapewniać centralne zarządzanie logami, umożliwiając przechowywanie, przetwarzanie i archiwizowanie dużej ilości logów z różnych źródeł w bezpieczny sposób.

- Powinien wspierać automatyczne przechowywanie i usuwanie logów zgodnie z politykami organizacji dotyczącymi retencji danych.

6. Zgodność z regulacjami

- System równoważny musi wspierać zgodność z regulacjami prawnymi i standardami branżowymi dotyczącymi monitorowania zdarzeń i logów, takimi jak RODO, SOX, HIPAA, PCI DSS oraz ISO/IEC 27001 lub równoważna.

- Powinien zapewniać mechanizmy szyfrowania i zabezpieczania danych zgodnie z wytycznymi dotyczącymi bezpieczeństwa informacji.

7. Integracja z istniejącą infrastrukturą

- System równoważny musi być w pełni kompatybilny z istniejącą infrastrukturą IT Zamawiającego, obejmującą serwery, systemy operacyjne (Windows, Linux, macOS), urządzenia sieciowe oraz aplikacje.

- Powinien oferować integrację z innymi narzędziami używanymi w infrastrukturze Zamawiającego, takimi jak systemy SIEM, monitoring wydajności (APM), narzędzia bezpieczeństwa (firewalle, IDS/IPS) oraz platformy zarządzania IT (np. Active Directory, LDAP).

8. Skalowalność

- System równoważny musi być skalowalny, zapewniając możliwość rozbudowy o dodatkowe źródła logów oraz rosnącą liczbę urządzeń i systemów, bez negatywnego wpływu na wydajność monitorowania.

- Powinien oferować możliwość monitorowania logów zarówno w małych, jak i dużych środowiskach IT, z możliwością dostosowania do przyszłych potrzeb Zamawiającego.

9. Zarządzanie użytkownikami i uprawnieniami

- System musi zapewniać możliwość zarządzania dostępem użytkowników na różnych poziomach, z możliwością przypisywania im odpowiednich ról oraz uprawnień.

- Administratorzy systemu muszą mieć możliwość dostosowania uprawnień dostępu do logów, konfiguracji systemu oraz generowania raportów w zależności od roli użytkownika.

10. Licencje

- System musi obejmować jedną dodatkową licencję na rozszerzenie monitorowania logów, która pozwoli na obsługę dodatkowych urządzeń, serwerów lub aplikacji w sieci Zamawiającego.

- Licencje powinny być elastyczne i skalowalne, umożliwiając rozbudowę systemu w przyszłości.

11. Wdrożenie i migracja

- W przypadku oferowania systemu lub jego równoważnego, Dostawca musi zapewnić pełne wdrożenie nowego/aktualizowanego systemu, w tym:

- Migrację istniejących danych i logów z dotychczasowego systemu.

- Konfigurację nowego systemu monitorowania zgodnie z politykami i wymaganiami Zamawiającego.

- Testy wdrożeniowe oraz optymalizację systemu w celu zapewnienia jego pełnej funkcjonalności.

12. Szkolenie

- Równoważny system musi być dostarczony wraz z odpowiednim szkoleniem dla administratorów systemu, obejmującym konfigurację monitoringu, zarządzanie logami oraz raportowanie.

- Szkolenie powinno obejmować również najlepsze praktyki dotyczące monitorowania logów oraz reagowania na alerty i incydenty.

13. Wsparcie techniczne

- System musi być wspierany przez producenta lub dostawcę, zapewniając regularne aktualizacje oprogramowania, poprawek bezpieczeństwa oraz wsparcie techniczne w przypadku problemów z systemem.

- Dostawca powinien oferować pomoc techniczną, konsultacje oraz wsparcie w zakresie konfiguracji i zarządzania systemem w długoterminowym okresie.

**[SYSTEM ZARZĄDZANIA ZGŁOSZENIAMI BŁĘDÓW]**

1 szt. licencji na system zarządzania zgłoszeniami błędów dla 40 użytkowników

Zamawiający wykorzystuje oprogramowanie Magik Info/Magik HelpDesk. Należy dostarczyć jedną licencję na rozszerzenie systemu lub system równoważny.

1. Zarządzanie zgłoszeniami

- Równoważny system musi umożliwiać pełne zarządzanie zgłoszeniami błędów, incydentów, problemów technicznych i próśb o wsparcie techniczne.

- System powinien obsługiwać kategoryzowanie zgłoszeń według typu problemu, priorytetu, działu odpowiedzialnego oraz statusu realizacji (otwarte, w toku, zamknięte).

- Musi zapewniać możliwość tworzenia, edytowania i zamykania zgłoszeń przez użytkowników i administratorów.

2. Śledzenie postępu zgłoszeń

- System równoważny musi umożliwiać śledzenie postępów każdego zgłoszenia, z możliwością przeglądania historii działań podejmowanych w ramach realizacji zgłoszenia.

- Powinien oferować funkcję powiadomień e-mail/SMS o zmianach w statusie zgłoszenia, zarówno dla użytkowników, jak i zespołów technicznych, aby informować o przydzieleniu, rozwiązaniu lub wymaganiu dodatkowych informacji.

3. Katalogowanie i baza wiedzy

- System musi umożliwiać tworzenie bazy wiedzy oraz katalogowanie najczęstszych problemów i rozwiązań. Użytkownicy powinni mieć możliwość przeszukiwania bazy wiedzy w celu samodzielnego rozwiązania problemów bez potrzeby zgłaszania incydentu.

- Powinna istnieć możliwość automatycznego sugerowania artykułów z bazy wiedzy na podstawie opisu problemu zgłoszonego przez użytkownika.

4. Obsługa wielokanałowa

- Równoważny system musi wspierać różne kanały zgłaszania problemów, w tym przez:

- Formularz internetowy,

- E-mail,

- Telefon,

- Aplikację mobilną.

- Musi umożliwiać centralizację zgłoszeń z różnych kanałów i ich przypisywanie do odpowiednich zespołów lub osób odpowiedzialnych.

5. Zarządzanie priorytetami i SLA

- System musi pozwalać na definiowanie i egzekwowanie poziomów SLA (Service Level Agreement) oraz priorytetów dla zgłoszeń na podstawie kryteriów takich jak typ problemu, poziom zagrożenia dla działalności organizacji czy czas odpowiedzi i rozwiązania zgłoszenia.

- Powinien automatycznie eskalować zgłoszenia, które nie zostały obsłużone w określonym czasie, zgodnie z ustalonymi poziomami SLA.

6. Raportowanie i analizy

- System równoważny musi oferować zaawansowane funkcje raportowania, w tym możliwość generowania raportów na temat:

- Liczby zgłoszeń w określonym przedziale czasowym,

- Średniego czasu rozwiązania problemów,

- Wydajności zespołów technicznych,

- Zgłoszeń w podziale na typy problemów, priorytety i inne kategorie.

- Raporty powinny być dostępne w formie graficznej i tabelarycznej, z możliwością eksportu do popularnych formatów, takich jak CSV, Excel, PDF.

7. Zarządzanie zespołem i przydzielanie zadań

- System musi wspierać zarządzanie zespołami technicznymi, umożliwiając przypisywanie zgłoszeń do konkretnych osób lub grup na podstawie ich umiejętności, dostępności lub lokalizacji.

- Musi umożliwiać ręczne i automatyczne przypisywanie zgłoszeń do odpowiednich działów lub specjalistów.

8. Integracja z innymi systemami

- Oprogramowanie równoważne powinno oferować możliwość integracji z innymi systemami używanymi przez Zamawiającego, takimi jak systemy ERP, CRM, narzędzia monitorowania infrastruktury IT czy bazy danych użytkowników.

- Integracja powinna obejmować automatyczne przekazywanie danych pomiędzy systemami, np. zgłoszeń, danych o użytkownikach, czy historii rozwiązywanych problemów.

9. Personalizacja i dostosowanie do procesów

- Równoważny system musi umożliwiać elastyczne dostosowanie interfejsu użytkownika oraz przepływów pracy (workflow) do specyficznych potrzeb i procesów Zamawiającego.

- Powinien pozwalać na definiowanie własnych formularzy zgłoszeń, pól danych oraz automatycznych procedur w oparciu o typ zgłoszenia lub jego kategorie.

10. Skalowalność i wydajność

- System równoważny musi być skalowalny, aby obsługiwać rosnącą liczbę zgłoszeń oraz użytkowników, nie wpływając na wydajność działania.

- Powinien zapewniać stabilne działanie zarówno w małych, jak i dużych organizacjach z różną ilością działów oraz zespołów wsparcia.

11. Bezpieczeństwo danych

- System musi zapewniać odpowiednie poziomy bezpieczeństwa, chroniąc zgłoszenia oraz dane użytkowników przed nieautoryzowanym dostępem. Wymagane jest wsparcie dla szyfrowania danych w ruchu i w spoczynku.

- System powinien umożliwiać zarządzanie uprawnieniami dostępu, pozwalając na przypisanie różnym użytkownikom odpowiednich ról i poziomów uprawnień.

12. Licencje

- Należy dostarczyć jedną licencję na rozszerzenie systemu lub w przypadku systemu równoważnego – licencję, która będzie zgodna z bieżącymi potrzebami Zamawiającego.

- Licencja musi obejmować możliwość obsługi wszystkich użytkowników, dla których jest wymagany dostęp do systemu zarządzania zgłoszeniami.

13. Wdrożenie i migracja

- W przypadku zaoferowania systemu równoważnego, Dostawca musi zapewnić pełne wdrożenie, które obejmuje:

- Migrację istniejących zgłoszeń, danych użytkowników oraz ustawień z dotychczasowego systemu.

- Konfigurację nowego systemu zgodnie z wymaganiami Zamawiającego.

- Testy działania systemu oraz optymalizację jego wydajności.

14. Szkolenie

- Dostawca musi zapewnić szkolenie dla administratorów systemu oraz zespołów wsparcia, obejmujące zarządzanie zgłoszeniami, konfigurowanie polityk i raportowanie.

- Szkolenie dla użytkowników końcowych (pracowników) powinno obejmować korzystanie z systemu do zgłaszania problemów oraz śledzenia statusu swoich zgłoszeń.

15. Wsparcie techniczne

- System musi być wspierany przez producenta lub dostawcę z dostępem do regularnych aktualizacji, poprawek bezpieczeństwa oraz wsparcia technicznego.

- Dostawca musi zapewnić dostęp do pomocy technicznej w przypadku problemów z systemem lub potrzeby konsultacji w zakresie konfiguracji.

Powyższy opis definiuje szczegółowe wymagania dotyczące rozszerzenia systemu zarządzania zgłoszeniami błędów lub systemu równoważnego dla rozwiązania Magik Info/Magik HelpDesk, zapewniając ciągłość działania i rozwój infrastruktury wsparcia technicznego.

**[****DLP. SYSTEM ZAPOBIEGAJĄCY WYCIEKOM DANYCH, MONITORUJĄCY OPERACJE NA KLUCZOWYCH PLIKACH]**

Zamawiający wykorzystuje oprogramowanie Safetica DLP, do istniejącego systemu należy dostarczyć 90 szt. licencji systemu zapobiegającego wyciekom danych lub system równoważny.

W przypadku dostarczenia dodatkowych licencji lub rozwiązania równoważnego dla systemu zapobiegającego wyciekom danych (DLP – Data Loss Prevention) oraz monitorującego operacje na kluczowych plikach, poniżej przedstawiono szczegółowy opis wymagań dla takiego systemu:

1. Zapobieganie wyciekom danych (DLP)

- Równoważny system musi oferować zaawansowane funkcje zapobiegania wyciekom danych, umożliwiając monitorowanie, kontrolowanie oraz blokowanie nieautoryzowanego przepływu danych w organizacji.

- System musi umożliwiać ochronę zarówno danych w spoczynku (na dyskach twardych, serwerach), jak i danych w ruchu (podczas przesyłania przez sieć) oraz danych w użyciu (np. podczas kopiowania na zewnętrzne nośniki lub drukowania).

- Należy zapewnić funkcjonalność pozwalającą na definiowanie polityk ochrony danych w oparciu o typy plików, ich zawartość, lokalizację oraz użytkownika.

2. Monitorowanie operacji na plikach

- System musi monitorować i rejestrować wszystkie operacje na plikach kluczowych dla Zamawiającego, takie jak: kopiowanie, przesyłanie, drukowanie, edytowanie, usuwanie oraz zmiany uprawnień.

- Musi zapewniać szczegółowe logi i audyty, które pozwolą na analizę działań użytkowników z plikami zawierającymi wrażliwe dane, zgodnie z polityką bezpieczeństwa.

3. Kontrola dostępu do danych

- System równoważny musi umożliwiać definiowanie i egzekwowanie zasad dostępu do danych na poziomie użytkownika, grup użytkowników lub działów organizacji, uwzględniając różne role i poziomy dostępu.

- Musi obsługiwać kontrolę uprawnień dostępu w zależności od kontekstu, takiego jak lokalizacja (wewnątrz organizacji, zdalnie), rodzaj urządzenia, oraz typ operacji na plikach.

4. Ochrona przed kopiowaniem i przesyłaniem danych

- System musi zapewniać możliwość blokowania lub monitorowania prób kopiowania danych na zewnętrzne urządzenia pamięci (np. USB, dyski zewnętrzne) oraz przesyłania danych przez e-mail, komunikatory, serwisy chmurowe (np. Dropbox, OneDrive) oraz inne kanały.

- Wymagane jest ścisłe monitorowanie i ewentualne blokowanie przesyłania danych poufnych poza organizację, z możliwością poddawania takich operacji kwarantannie lub autoryzacji przez administratora.

5. Zgodność z regulacjami

- System musi być zgodny z obowiązującymi regulacjami dotyczącymi ochrony danych osobowych i bezpieczeństwa informacji, takimi jak RODO, ISO 27001, oraz innymi standardami branżowymi, odpowiednimi dla specyfiki działalności Zamawiającego.

- Musi wspierać klasyfikację danych i automatyczne stosowanie odpowiednich polityk ochrony na podstawie zawartości danych (np. dane osobowe, finansowe, tajemnice przedsiębiorstwa).

6. Raportowanie i analiza zagrożeń

- System równoważny musi oferować zaawansowane funkcje raportowania i analizy, w tym możliwość generowania raportów z operacji na plikach oraz incydentów bezpieczeństwa.

- Musi posiadać mechanizmy automatycznego wykrywania potencjalnych zagrożeń (np. nietypowe operacje na plikach, próby nieautoryzowanego dostępu) i ostrzegania administratorów w czasie rzeczywistym.

7. Integracja z istniejącą infrastrukturą

- Równoważne rozwiązanie musi być w pełni kompatybilne z istniejącą infrastrukturą IT Zamawiającego, w tym systemami operacyjnymi, serwerami, stacjami roboczymi oraz istniejącymi systemami monitorowania i zarządzania bezpieczeństwem.

- Powinno wspierać integrację z innymi narzędziami używanymi do monitorowania i ochrony, takimi jak systemy SIEM (Security Information and Event Management), platformy klasyfikacji danych oraz oprogramowanie antywirusowe.

8. Licencje

- System musi obejmować 90 dodatkowych licencji dla użytkowników, z możliwością ich elastycznego przydzielania i zarządzania w ramach jednego centralnego systemu.

- Licencje powinny pozwalać na skalowanie systemu w przyszłości, w przypadku potrzeby ochrony większej liczby użytkowników i urządzeń.

9. Wdrożenie i migracja

- Dostawca musi zapewnić pełne wdrożenie oferowanego rozwiązania równoważnego, w tym:

- Odinstalowanie lub integrację z dotychczasowym systemem ochrony przed wyciekiem danych.

- Instalację i konfigurację nowego systemu, w tym migrację istniejących polityk bezpieczeństwa oraz danych z dotychczasowego rozwiązania.

- Testy działania systemu i jego optymalizację w celu zapewnienia płynnego działania bez zakłóceń dla użytkowników.

10. Szkolenie

- Równoważny system musi być dostarczony wraz z:

- Certyfikowanym szkoleniem dla administratorów systemu, które obejmie konfigurację, zarządzanie i monitorowanie operacji na plikach oraz ochronę danych przed wyciekiem.

- Szkolenie dla użytkowników końcowych, które może być w formie self-learningu, dotyczące najlepszych praktyk pracy z plikami oraz przestrzegania polityk bezpieczeństwa.

11. Wsparcie techniczne i aktualizacje

- Oferowane rozwiązanie musi obejmować wsparcie techniczne producenta lub dostawcy, z dostępem do regularnych aktualizacji oprogramowania, poprawek bezpieczeństwa oraz asysty technicznej w przypadku problemów.

- System musi być stale aktualizowany w celu spełniania najnowszych wymogów bezpieczeństwa oraz zgodności z regulacjami.

Powyższy opis zawiera wymagania dla równoważnego rozwiązania do zapobiegania wyciekom danych oraz monitorowania operacji na plikach, które może zastąpić lub uzupełnić obecnie wykorzystywany system.

**[OPROGRAMOWANIE WSPIERAJĄCE KONTROLĘ]**

1 szt. licencji na oprogramowanie dla 40 użytkowników Wolters Kluwer LEX Kontrola zarządcza Plus

Zamawiający wykorzystuje obecnie oprogramowanie Wolters Kluwer LEX Kontrola zarządcza Plus, należy dostarczyć dodatkową licencję lub system równoważny.

Równoważny systemu musi obejmować zaawansowane funkcje:

1. Dostawę oprogramowania/system do Kontroli Zarządczej

2. Szkolenie z funkcjonowania wszystkich elementów systemu dla użytkowników

3. Analiza wdrożeniowa na podstawie dokumentów budżetu na 2025 r. Regulaminu organizacyjnego itp. w tym zidentyfikowanie i wprowadzenie do dostarczonego systemu danych do funkcjonowania systemu kontroli zarządczej w urzędzie w 2025r.

Oprogramowanie umożliwiające jednostkom samorządu terytorialnego (JST) realizację obowiązku kontroli zarządczej wynikającej z art. 68 ustawy o finansach publicznych tj.:

- stałe badanie zgodności swoich działań z przepisami prawa,

- zarządzanie ryzykiem,

- usprawnienie przepływu informacji w zakresie działalności jednostki,

- monitorowanie etapów prac wraz z szybką analizą zgromadzonych danych.

System, wspiera pracę kierownictwa i pracowników JST w realizacji obowiązków wynikających z kontroli zarządczej. Skuteczne narzędzie przygotowania jednostki do kontroli zewnętrznych i audytu.

Główne funkcjonalności systemu:

A. Określanie planów działalności

1. Umożliwia przygotowanie planu działalności jednostki lub komórki organizacyjnej oraz przygotowanie sprawozdania z jego wykonania.

2. Umożliwia przypisanie zadania do wyznaczonych celów strategicznych i operacyjnych ze wskazaniem osoby odpowiedzialnej za wykonanie zadania wraz z ryzykami, które mogą wpłynąć na realizację tych zadań.

3. Umożliwia określenie mierników do wskazanych celów przypisanych do danego planu działalności.

4. Pozwala na bieżące monitorowanie wykonywania planu oraz oceny ryzyka.

B. Zarządzanie ryzykiem

1. Umożliwia kontrolowanie całego procesu związanego z zarządzaniem ryzykiem, począwszy od identyfikacji ryzyka poprzez jego ocenę i określenie sposobu postępowania w rejestrze, aż do momentu wygenerowania mapy ryzyka.

2. Umożliwia w szczególności:

a) Definiowanie oraz bieżącą aktualizację rejestru ryzyka w jednostce;

b) Zgłaszanie ryzyka przez każdego użytkownika systemu;

c) Powiązanie ryzyka z wyznaczonymi zadaniami zawartymi w Planie działalności (z poziomu planu);

d) Przypisanie ryzyka do właściciela oraz zapewnienie komunikacji między właścicielami i managerem.

e) Zarządzanie ryzykiem w sposób systemowy,

f) Realizację ustawowego obowiązku w obszarze zarządzania ryzykiem,

g) Przekazywanie kierownictwu jednostki rzetelnej informacji o ryzyku,

h) Formułowanie wstępnych decyzji o charakterze zarządczym, na podstawie wygenerowanej analizy ryzyka z systemu,

i) Przygotowanie mapy ryzyka, która jest graficzną prezentacją ryzyka w momencie pierwotnym i po zastosowaniu mechanizmów redukujących ryzyko.

C. Lista pytań kontrolnych

1. Pozwala przeprowadzać bieżące badania zgodności z przepisami prawa i innymi regulacjami na podstawie list pytań kontrolnych.

2. Pozwala tworzyć własne listy pytań kontrolnych lub korzystać z gotowych list przygotowanych przez ekspertów z danej dziedziny.

3. Umożliwia tworzenie przez użytkownika własnych list kontrolnych uwzględniających wagowanie istotności pytań i odpowiedzi.

4. Umożliwia integrację z systemem informacji prawnej i powiązane z jednostką redakcyjną podstawy prawnej lub orzeczenia, do której odwołują się poszczególne pytania w listach;

5. Dostawca systemu na bieżąco aktualizuje listy kontrolne – zgodnie ze zmieniającymi się przepisami prawa.

6. Prezentacja wyników z wykonanych badań zgodności dostępna jest w przejrzystej formie, z wyszczególnieniem wszystkich zidentyfikowanych niezgodności z możliwością pobranie pliku pdf lub xlsx.

7. Listy kontrolne dostępne są do następujących dziedzin:

a) Zamówienia publiczne,

b) Cyberbezpieczeństwo,

c) Normy ISO,

d) Architektura i budownictwo,

e) RODO,

f) Finanse publiczne w jednostkach samorządu terytorialnego

g) Rachunkowość

h) Funkcjonowanie urzędu w czasie pandemii.

8. Przygotowanie raportu z wykonywanych badań zgodności, w których parametrem będzie poziom zgodności.

D. Zadania

1. Umożliwia zarządzanie procesami przeprowadzania badań zgodności przez:

a) Zdalne wydawanie poleceń wykonania analizy, badania, raportu, sprawozdania użytkownikom wskazanym w organizacji oraz w jednostkach podległych,

b) Zlecanie zadań (w tym zadań cyklicznych) do użytkowników na każdym poziomie organizacji,

c) Przekazywanie zadań z załączoną listą pytań kontrolnych lub ankietą do użytkowników na każdym poziomie odpowiedzialności,

d) Dołączanie do delegowanych zadań plików z wewnętrznymi procedurami placówki,

e) Automatyczne powiadamianie użytkowników (wskazanych w poleceniu) o konieczności przygotowania sprawozdania, wypełnienia listy kontrolnej lub ankiety.

2. Moduł umożliwia ponadto:

a) Sprawdzanie zgodności działania jednostki/komórki organizacyjnej z obowiązującym prawem lub regulacjami wewnętrznymi (w połączeniu z modułem checklist);

b) Reagowanie na ryzyko niezgodności poprzez delegowanie pracownikom konkretnych zadań redukujących niezgodności i śledzących skuteczność ich wykonania;

c) Bieżący monitoring wykonanych zadań;

3. Moduł umożliwia raportowanie realizowanych w placówce zadań i projektów we wszystkich obszarach i obowiązkach, wynikających z funkcjonowania jednostek samorządu terytorialnego.

4. System prezentuje dwa rodzaje raportów - raporty statystyczne i przeglądowe, które umożliwiają:

a) Ustalenie, jakie sprawozdania zostały wykonane w systemie;

b) Ustalenie ilości zadań i sprawozdań względem użytkowników albo obowiązków;

c) Monitorowanie wykonania zadań z uwzględnieniem kryterium obowiązku.

E. Ankiety

1. Wspiera w bieżącym utrzymaniu zgodności poprzez:

a) Tworzenie ankiet zawierających pytania jednokrotnego, wielokrotnego wyboru oraz pytania otwarte;

b) Kreatora ankiet ułatwiających przygotowanie ankiety i analizatora ankiet ułatwiającego przygotowanie wyników do analizy i oceny;

c) Włączenie opcji anonimowej ankiety oraz możliwości wielokrotnego wykonania ankiety;

d) Możliwość wygenerowania linku do ankiety ankiety np. do umieszczenia na stronie internetowej.

F. Zarządzanie zdarzeniami organizacyjnymi (Niezgodnościami)

1. Umożliwia nadzór nad zdarzeniami organizacyjnymi nadzorowanymi przez wyznaczone osoby określone na poziomie globalnym;

2. Zarządzania zdarzeniami organizacyjnymi pozwala na:

a) Definiowanie indywidualnych słowników zdarzeń;

b) Przypisywanie globalnie właścicieli do kategorii zdarzeń;

c) Włączenie anonimowości zgłoszeń;

d) Tworzenie rejestr niezgodności;

e) Śledzenie historii zmian zdarzeń organizacyjnych

f) Identyfikacji ryzyka z poziomu zgłoszonego zdarzenia organizacyjnego;

g) Wyznaczenie zadań korygujących i naprawczych z poziomu zdarzenia;

h) Przygotowanie zgłoszenia do Urzędu w zakresie naruszeń ochrony danych osobowych.

G. Komunikaty

1. Moduł umożliwia przesyłanie ogłoszeń i wiadomości do użytkowników systemu, zarówno w organizacji jak i w jednostkach podległych,

2. Moduł umożliwia wygenerowanie raportu potwierdzenia przeczytania komunikatu zawierającego listę osób oraz czas odczytania ogłoszenia lub wiadomości,

3. Moduł ułatwia przekazywanie informacji np. o nowych aktach wewnętrznych i ich przesyłanie z bezpośrednim linkiem do repozytorium dokumentów.

H. RODO

a) umożliwia zgłaszanie naruszeń ochrony danych osobowych

b) prowadzenie rejestru RODO

c) prowadzenie listy kontrolnej RODO

I. Współpraca/integralność systemu - automatyzuje badania zgodności z prawem w zakresie przepisów ochrony danych osobowych (RODO) oraz pozwala na:

1. Prowadzenie rejestrów:

a) Rejestr czynności przetwarzania

b) Rejestr dokumentów powierzenia

c) Rejestr zgód

d) Rejestr udostępnień i zapytań

e) Rejestr ocen skutków wpływu na prywatność

f) Rejestr incydentów

2. Zgłaszanie naruszeń związanych z ochroną danych osobowych przez każdego pracownika placówki, ich rejestrowanie oraz generowanie zgłoszenia do Urzędu Ochrony Danych Osobowych.

3. Zarządzanie zgłoszonymi naruszeniami pozwala na:

a) Dodawanie zgłoszonego incydentu do rejestru;

b) Komentowanie zdarzeń w rejestrze;

c) Wysyłanie zadania z poziomu zgłoszonego incydentu przez uprawnionych użytkowników;

d) Śledzenie historii zmian zgłoszonego naruszenia.

4. Przeprowadzanie badań zgodności przy użyciu list pytań kontrolnych w zakresie rozporządzenia RODO

**[SYSTEM ZARZĄDZANIA DOSTĘPEM DO SIECI NA POZIOMIE UŻYTKOWNIKÓW]**

1 szt. licencji na oprogramowania dla 150 urządzeń sieciowych NACVIEW NAC

Zamawiający wykorzystuje oprogramowanie NACVIEW w swojej sieci, należy dostarczyć dodatkową licencję lub system równoważny.

1. Zarządzanie dostępem do sieci

- Równoważne oprogramowanie musi zapewniać pełną kontrolę dostępu do sieci, tak jak obecnie wykorzystywane rozwiązanie. Oznacza to możliwość:

- Identyfikacji, autoryzacji oraz kontrolowania urządzeń i użytkowników łączących się z siecią.

- Wymuszania odpowiednich polityk bezpieczeństwa i segmentacji sieci w oparciu o zdefiniowane kryteria, takie jak typ urządzenia, użytkownik, rola w organizacji, lokalizacja czy stan zabezpieczeń urządzenia (compliance).

2. Obsługa wielu rodzajów urządzeń

- Oprogramowanie równoważne musi umożliwiać zarządzanie dostępem zarówno dla urządzeń przewodowych, jak i bezprzewodowych.

- Powinno wspierać szeroką gamę urządzeń końcowych, w tym komputerów stacjonarnych, laptopów, smartfonów, tabletów oraz urządzeń IoT.

3. Zgodność z istniejącą infrastrukturą

- Równoważne rozwiązanie musi być w pełni kompatybilne z obecną infrastrukturą sieciową, w tym z przełącznikami sieciowymi, punktami dostępu Wi-Fi, systemami firewall oraz serwerami.

- Powinno obsługiwać popularne protokoły sieciowe i autoryzacyjne, takie jak 802.1X, RADIUS, TACACS+ oraz integracje z systemami typu Active Directory, LDAP czy inne bazy użytkowników wykorzystywane w sieci Zamawiającego.

4. Monitorowanie i raportowanie

- Oprogramowanie musi oferować możliwość monitorowania wszystkich aktywności w sieci w czasie rzeczywistym, w tym aktywności użytkowników oraz urządzeń.

- Powinno zapewniać zaawansowane funkcje raportowania oraz alarmowania, w tym możliwość generowania raportów dotyczących zgodności z politykami, statystyk urządzeń oraz zagrożeń sieciowych.

- Możliwość tworzenia niestandardowych raportów na potrzeby audytów oraz analiz bezpieczeństwa.

5. Zarządzanie politykami dostępu

- System równoważny musi umożliwiać tworzenie i egzekwowanie złożonych polityk dostępu do sieci, w tym dynamiczne przypisywanie uprawnień na podstawie kryteriów takich jak rola użytkownika, grupa, stan bezpieczeństwa urządzenia (np. aktualność oprogramowania, zainstalowane oprogramowanie antywirusowe).

- Równoważne oprogramowanie powinno również obsługiwać polityki dostępu opartych na czasie (np. dostęp tylko w określonych godzinach) oraz lokalizacji (segmentacja VLAN, dostęp w zależności od lokalizacji w sieci).

6. Zarządzanie zagrożeniami

- Równoważne rozwiązanie musi oferować funkcje zarządzania zagrożeniami, takie jak wykrywanie i blokowanie nieautoryzowanych lub niebezpiecznych urządzeń w sieci.

- Oprogramowanie powinno mieć możliwość integracji z innymi narzędziami zabezpieczającymi (takimi jak systemy IDS/IPS, firewalle, rozwiązania SIEM), aby umożliwić skoordynowane działania w zakresie zarządzania incydentami i reagowania na zagrożenia.

7. Łatwość wdrożenia i skalowalność

- Równoważne oprogramowanie powinno być łatwe do wdrożenia i zarządzania, oferując intuicyjny interfejs administracyjny z możliwością centralnego zarządzania.

- System musi być skalowalny, pozwalając na elastyczne dodawanie nowych urządzeń i użytkowników bez utraty wydajności czy stabilności sieci.

8. Licencje

- Równoważne oprogramowanie musi obejmować licencje pozwalające na zarządzanie taką samą liczbą urządzeń i użytkowników jak dotychczasowe rozwiązanie, z możliwością rozbudowy w przyszłości w zależności od potrzeb Zamawiającego.

9. Wdrożenie i migracja

- W przypadku oferowania rozwiązania równoważnego, Dostawca musi zapewnić pełne wdrożenie, które obejmuje:

- Odinstalowanie lub zastąpienie dotychczasowego rozwiązania na urządzeniach.

- Instalację i konfigurację nowego oprogramowania, w tym migrację wszelkich polityk i ustawień, tak aby nowy system działał w sposób płynny i bez zakłóceń dla użytkowników sieci.

- Testy poprawności działania i integracji z istniejącą infrastrukturą sieciową.

10. Szkolenie

- Oferowane rozwiązanie równoważne musi być dostarczone wraz z:

- Certyfikowanym szkoleniem dla administratorów systemu (przynajmniej 2 osoby). Szkolenie to powinno obejmować pełne zarządzanie rozwiązaniem, w tym konfigurację, monitorowanie i optymalizację systemu.

- Szkolenie dla użytkowników końcowych, które może mieć formę self-learningu lub dokumentacji użytkowej, w celu zapoznania ich z funkcjami dotyczącymi dostępu do sieci.

11. Wsparcie techniczne

- Nowe rozwiązanie musi być wspierane przez producenta lub dostawcę, oferując wsparcie techniczne w zakresie konfiguracji, aktualizacji oprogramowania oraz rozwiązywania problemów technicznych.

- Dostawca musi zapewnić dostęp do regularnych aktualizacji oraz poprawek zabezpieczeń.

12. Certyfikacja i zgodność

- Oprogramowanie musi posiadać odpowiednie certyfikaty branżowe, takie jak zgodność z wymaganiami RODO, PCI DSS, ISO/IEC 27001 oraz innymi, zgodnie z regulacjami stosowanymi w organizacji Zamawiającego.

Powyższy opis definiuje szczegółowe wymagania dla równoważnego systemu NAC, który miałby zastąpić lub uzupełnić dotychczas testowane rozwiązanie wykorzystywane przez Zamawiającego.

**[OPROGRAMOWANIE ANTYWIRUSOWE]**

80 szt. licencji w tym 5 serwerów oprogramowania ESET Protect Elite

Minimalne wymaganie:

Zamawiający wykorzystuje obecnie oprogramowanie ESET. Należy dostarczyć licencje pozwalające rozszerzyć funkcjonalność posiadanego rozwiązania łącznie do 80 licencji dla użytkowników w tym 5serwerów, wykonać analizę funkcjonalno-użytkową stosowanego rozwiązania, w razie potrzeby przeprowadzić konfigurację i optymalizację stosowanego rozwiązania na wszystkich stanowiskach, testy poprawności działania i integracji z infrastrukturą Zamawiającego, szkolenie dla 4 administratorów

Wymagane jest zarządzanie dostarczonym rozwiązaniem z posiadanej przez Zamawiającego konsoli administracyjnej ESET

W przypadku zaoferowania rozwiązania równoważnego Dostawca zobowiązany jest do dostarczenia: rozwiązania równoważnego dla wszystkich 80 użytkowników/końcówek/serwerów wraz z wdrożeniem, wymianą (odinstalowaniem ESET i zainstalowaniem nowego oprogramowania) na końcówkach/serwerach oraz certyfikowanym przez producenta szkoleniem dla 4 administratorów oraz szkoleniem dla użytkowników (może być selflearning).

1. Zarządzanie i integracja

- Równoważne rozwiązanie musi być w pełni kompatybilne z istniejącą konsolą administracyjną ESET, lub alternatywnie, nowa konsola administracyjna musi zostać dostarczona, wdrożona i skonfigurowana przez Dostawcę, wraz z odpowiednią migracją danych z obecnej konsoli.

- W przypadku braku możliwości integracji z konsolą ESET, Dostawca musi zapewnić rozwiązanie, które umożliwi centralne zarządzanie wszystkimi 80 licencjami dla użytkowników lub serwerów, oferując przynajmniej takie same funkcje jak konsola ESET.

2. Funkcjonalność ochrony

- Równoważne oprogramowanie musi oferować co najmniej takie same funkcje jak obecnie używany ESET. Należy więc zapewnić m.in.:

- Ochronę przed wirusami, ransomware, malware, spyware, phishingiem.

- Ochronę na poziomie systemu plików, poczty elektronicznej oraz przeglądarek internetowych.

- Ochronę serwerów oraz końcowych stacji roboczych.

- Skuteczne zarządzanie zagrożeniami w czasie rzeczywistym oraz automatyczne aktualizacje.

3. Licencje

- Nowe oprogramowanie musi obejmować co najmniej 80 licencji dla użytkowników, końcówek lub 5 serwerów.

- Licencje muszą być zgodne z bieżącymi potrzebami Zamawiającego, czyli pozwalać na zarządzanie z poziomu jednej centralnej konsoli administracyjnej i być przypisane zarówno do komputerów, jak i serwerów.

4. Wdrożenie

- Oferowane rozwiązanie równoważne musi obejmować pełne wdrożenie, które uwzględnia:

- Odinstalowanie istniejącego oprogramowania ESET na końcówkach oraz serwerach.

- Instalację nowego oprogramowania na tych samych urządzeniach.

- Konfigurację i optymalizację nowego rozwiązania.

- Testy poprawności działania i integracji z infrastrukturą Zamawiającego.

5. Szkolenie

- Równoważne oprogramowanie musi być dostarczone wraz z:

- Certyfikowanym przez producenta szkoleniem dla 4 administratorów. Szkolenie to musi obejmować pełne zarządzanie rozwiązaniem, w tym instalację, konfigurację, monitorowanie, reagowanie na zagrożenia oraz wszelkie procedury związane z administracją systemem.

- Szkolenie dla użytkowników końcowych, które może przyjąć formę self-learningu, aby umożliwić użytkownikom szybkie zapoznanie się z funkcjami oprogramowania, takimi jak postępowanie w przypadku wykrycia zagrożenia.

6. Certyfikacja i zgodność

- Oferowane rozwiązanie musi posiadać odpowiednie certyfikaty oraz spełniać standardy bezpieczeństwa, zgodnie z wymaganiami branżowymi i prawnymi.

- Wszelkie procesy związane z wymianą, wdrożeniem i zarządzaniem nowym oprogramowaniem muszą być przeprowadzone zgodnie z najlepszymi praktykami oraz standardami bezpieczeństwa IT.

7. Wsparcie techniczne

- Nowe rozwiązanie musi być wspierane przez producenta lub dostawcę, z zapewnieniem wsparcia technicznego co najmniej na poziomie obecnego wsparcia oferowanego przez ESET.

- Dostępność aktualizacji oraz poprawek zabezpieczeń musi być zapewniona w cyklu regularnym i dostosowana do wymagań Zamawiającego.

8. Testy i pilotaż

- Zamawiający może wymagać okresu testowego (np. pilotażowego wdrożenia) nowego rozwiązania równoważnego przed pełnym wdrożeniem na 80 stanowiskach, aby ocenić jego wydajność, skuteczność i integrację z istniejącą infrastrukturą IT.

9. Koszty

- Oferent równoważnego rozwiązania musi przedstawić pełną kalkulację kosztów, wliczając w to licencje, wdrożenie, szkolenia, wsparcie techniczne oraz ewentualną wymianę konsoli administracyjnej, jeśli dotychczasowa konsola ESET nie będzie zgodna z nowym oprogramowaniem.