**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 40 kW, 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.

**[SYSTEM ZABEZPIECZEŃ DANYCH]**

1x serwer fizyczny NAS

Minimalne wymagania:

1. Urządzenie musi zostać dostarczone ze wszystkimi komponentami do zabudowy w standardowej szafie rack 19", w obudowie typu rack o wysokości nie większej niż 2U.

2. Urządzenie NAS musi posiadać nadmiarowy zasilacz

3. Urządzenie umożliwia zainstalowanie minimum 12 dysków 3,5" SATA HDD lub 2,5" SATA SSD, oraz do 36 dysków z rozszerzeniem

4. Urządzenie musi zawierać łącznie nie mniej niż 144 TB zainstalowanej pojemności z wykorzystaniem minium 12 identycznych 3.5" dysków HDD o pojemności 12 TB i przepustowości 6 Gbit/s każdy

5. Urządzenie pozwala na wymianę dysku podczas jego pracy

6. Urządzenie posiada minimum 16 GB pamięci RAM, rozszerzalnej do 64 GB (DDR4).

7. Urządzenie powinno posiadać minimum następujące porty zewnętrzne:

7.1 4x RJ-45 1GbE

7.2 2x RJ-45 10GbE

7.3 2x USB 3.2.1

7.4 2x inifiniband

8. Urządzenie musi zapewniać poziom zabezpieczenia danych na dyskach następującymi poziomami RAID: JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10

9. Urządznie posiada 2x slot PCIe Gen3 x8

10. Procesor urządzenia powinien być 64 bitowy i osiągać wynik nie mniejszy niż 10100 w testach PassMark https://www.cpubenchmark.net/

11. Oferowany serwer NAS musi być fabrycznie nowy, Urządzenie musi pochodzić z legalnego kanału sprzedaży producenta na terenie Unii Europejskiej i reprezentuje model bieżącej linii produkcyjnej.

Nie dopuszcza się użycia macierzy lub jej elementów - odnawianych, demonstracyjnych lub powystawowych

12. Urządzenie wspiera migrację RAID z RAID1 na RAID5, z RAID5 na RAID6

12. Urządzenie wspiera migrację RAID z RAID1 na RAID5, z RAID5 na RAID6

13. Urządzenie wspiera powiększanie wolumenu za pomocą większych dysków w konfiguracji: RAID:1/5/6/10

14. Urządzenie wspiera rozszerzenie wolumenu poprzez dodanie dysków twardych w konfiguracji: JBOD, RAID:5/6

15. Urządzenie wspiera Dysk Hot Spare w konfiguracji RAID:1/5/6/10

16. Urządzenie udostępnia przestrzeń przez minimum następujące protokoły plikowe: SMB, AFP, NFS, FTP, WebDAV, Rsync

17. Urządzenie posiada wsparcie dla integracji listy kontroli dostępu systemu Windows (ACL)

18. Urządzenie można konfigurować przy użyciu przeglądarek WWW m.in Chrome, Firefox, Edge, Safari

19. W urządzeniu jest zainstalowany adapter na dyski M.2 NVMe, wraz z dwoma dyskami NVMe SSD 800 GB każdy

**[SYSTEM REDUNDANCJI W CHMURZE]**

Przedmiotem zamówienia jest rozwiązanie kopii danych do 10 TB w chmurze publicznej jako zabezpieczenie DR na okoliczność incydentów cybernetycznych i fizycznych, lokalizacja danych - Polska. Usługa na okres do 30 czerwca 2026.

1. Usługa musi oferować wysoce dostępny, wysoce skalowalny, trwały i bezpieczny magazyn dla różnych obiektów danych w chmurze publicznej.

2. Obiekty danych muszą być dostępne z dowolnego miejsca na świecie za pośrednictwem protokołu HTTP lub HTTPS oraz za pośrednictwem interfejsu API REST.

3. Usługa powinna również oferować biblioteki klienckie dla deweloperów tworzących aplikacje lub usługi za pomocą platformy .NET, Java, Python, JavaScript, C++i Go.

4. Deweloperzy i specjaliści IT muszą mieć możliwość używania komend i skryptów programu PowerShell.

5. Dostęp do zarządzania usługą powinna być z poziomu witryny internetowej i dedykowanego oprogramowania.

6. Przedmiot zamówienia powinien odznaczać się następującymi cechami:

6.1 niezawodność i wysoka dostępność uzyskana dzięki kopiom i replikom. Tak uzyskana nadmiarowość powinna zapewnić bezpieczeństwo danych w przypadku przejściowych awarii sprzętu. Replikacja powinna być dostępna na poziomie centrów przetwarzania danych i/lub regionów geograficznych.

6.2 posiada mechanizm szyfrowania danych w celu zapewnienia bezpieczeństwa

6.3 usługa musi być zaprojektowana jako wysoce skalowalne rozwiązanie spełniające potrzeby związane z magazynowaniem danych i wydajnością współczesnych aplikacji.

6.4 dostępność na poziomie globalnym. Dane muszą być dostępne z dowolnego miejsca na świecie za pośrednictwem protokołu HTTP lub HTTPS. Biblioteki klienckie muszą być dostępne w różnych językach, w tym .NET, Java, Node.js, Python, Go i innych. Usługa musi być także kompatybilna z interfejsem API REST. Usługa musi obsługiwać skrypty programu PowerShell lub interfejsu wiersza poleceń. Praca z danymi powinna się odbywać albo za pośrednictwem dedykowanej witryny internetowej, albo dedykowanego oprogramowania.

7. Przedmiot zamówienia musi zawierać następujące usługi:

7.1 wysoce skalowalny magazyn obiektów dla danych tekstowych i binarnych do obsługi i analizy danych big data

7.2 zarządzane udziały plików dla wdrożeń lokalnych lub w chmurze.

7.3 magazyn obsługi komunikatów zapewniający niezawodną obsługę komunikatów między składnikami aplikacji.

7.4 magazyn obiektów NoSQL do magazynowania ustrukturyzowanych danych bez użycia schematu.

7.5 usługi zarządzania woluminami, wdrażania i aranżacji utworzone natywnie dla kontenerów.

7.6 każda z wymienionych usług musi być dostępna za pośrednictwem konta magazynu z unikatowym adresem.

8. Dostawca usługi musi gwarantować możliwość wyboru lokalizacji przechowywania danych przynajmniej w 5 lokalizacjach w Europie.

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

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

Poniżej znajduje się opis dla 1 urządzenia. Zamawiający wymaga dostawy 4 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), 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 16Gb/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. 20 Gbps, wydajność przełączania przynajmniej 15 Mpps

7. Obsługa min. 16 000 adresów MAC

8. Wbudowana pamięć RAM min. 256MB. Procesor wielordzeniowy. Minimalne taktowanie procesora 800MHz

9. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB

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

11. Możliwość skonfigurowania min. 32 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. 1 000 tras dla routingu IPv4

21. Obsługa min. 200 tras dla routingu IPv6. Obsługa min. 200 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 1 000 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 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 5 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. 128 Gbps, wydajność przełączania przynajmniej 95 Mpps

7. Obsługa min. 16 000 adresów MAC

8. Wbudowana pamięć RAM min. 256MB. Procesor wielordzeniowy. Minimalne taktowanie procesora 800MHz

9. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB

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

11. Możliwość skonfigurowania min. 32 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. 1 000 tras dla routingu IPv4

21 Obsługa min. 200 tras dla routingu IPv6

21.1 Obsługa min. 200 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 1 000 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 5 cm

3.3 możliwość zasilania przez zasilacz DC

3.4 zakres temperatur pracy ciągłej co najmniej 0°C – +50°C

3.5 zakres wilgotności pracy co najmniej 5% - 90%

3.6 waga nie większa niż 0,6kg

4. Punkt dostępowy musi posiadać:

4.1 dedykowany port konsolowy

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

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 6dBi 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 5.0

12. Zużycie mocy nie większe niż 14W

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

15. Urządzenie musi posiadać standard bezpieczeństwa EN62368-1

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

17.9 MLD Snooping i IGMP Snooping

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:

1. Informacje ogólne

1.1 Urządzenie musi być fabrycznie nowe i nieużywane przed dniem dostarczenia do siedziby Zamawiającego, z wyłączeniem użycia niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

2. Obudowa

2.1 Obudowa typu RACK o wysokości minimalnej 2U

2.2 Możliwość instalacji min. 8 dysków 2,5” Hot-Plug

2.3 Obudowa wyposażona w panel diagnostyczny lub sygnalizację LED umieszczoną na froncie obudowy informująca o stanie serwera.

2.4 Musi być wyposażona w przednią ramkę, zamykaną na klucz, chroniącą dyski przed nieuprawnionym wyjęciem. Ramka musi umożliwiać włączenie i wyłączenie podświetlenia umożliwiając lepszą identyfikację serwera.

2.5 Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Ramię do zarządzania przewodami.

3. Płyta główna

3.1 Płyta główna z możliwością zainstalowania minimum dwóch procesorów

3.2 Obsługa minimum 4 TB RAM. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM DDR5.

4. Procesor

4.1 Dwa procesory wielordzeniowe osiągające w teście PassMark CPU Mark wynik min. 49.000 pkt według danych ze strony https://www.cpubenchmark.net/multi\_cpu.html dla konfiguracji wieloprocesorowej.

5. Pamięć ram

5.1 Zainstalowana pamięć RAM minimum 512 GB RDIMM DDR5 lub LRDIMM.

5.2 Rozmiar pojedynczej kości pamięci RAM 32GB.

5.3 Możliwość rozbudowy do minimum 1,5 TB.

5.4 Memory mirroring, ECC, patrol scrubbing, SDDC, memory thermal throttling, ADDDC-SR, PPR, Memory SMBus hang recovery.

6. Pamięć masowa

6.1 Minimum 6 dysków 1.92TB SSD typu HotPlug

6.2 Możliwość instalacji dysków twardych SATA, SAS, SSD.

6.3 Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego.

7. Kontroler

7.1 Sprzętowy kontroler dyskowy RAID obsługujący poziomy 0, 1, 5, 6, 10, 50, 60, wyposażony w pamięć cache o pojemności min. 8GB oraz podtrzymanie bateryjne.

8. Karta graficzna

8.1 Zintegrowana karta graficzna o rozdzielczości minimum 1920x1200

9. Wbudowane porty

9.1 Minimum 2 porty USB wersji 3.0 lub nowszej.

9.2 1 Port USB TYP-C na przednim panelu obudowy, musi umożliwiać dostęp do modułu zarządzania serwerem poprzez bezpośrednie połączenie.

9.3 Minimum 1 port VGA.

10. Interfejsy sieciowe

10.1 Dwa interfejsy 10Gb w standardzie Base-T.

10.2 Sumarycznie minimum cztery interfejsy sieciowe 10 GbE wraz z wkładkami SFP+, zapewnione przez minimum 2 karty sieciowe (Po 2 interfejsy 10 GbE SFP+ na jednej karcie sieciowej).

10.3 Jeden interfejs 1Gb w standardzie Base-T do zarządzania serwerem.

11. Zasilanie

11.1 Redundantne zasilacze Hot Plug, każdy o mocy minimum 1600W Titanium, pracujące w sieci 230V 50/60Hz prądu zmiennego.

12. Wentylatory

12.1 Redundantne wentylatory typu Hot-Plug.

13. Bezpieczeństwo

13.1 Zintegrowany z płytą główną moduł TPM 2.0.

14. Zarządzanie

14.1 Moduł umożliwiający zdalne zarządzanie serwerem.

14.2 Oprogramowanie do zdalnego zarządzania serwerem, zapewniające minimum: monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), monitorowanie w czasie rzeczywistym poboru prądu przez serwer, zbieranie logów błędów hardware, przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, montowanie wirtualnych napędów, zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, wysyłanie zawiadomień droga mailową i poprzez SNMP. Wsparcia dla IPMI, SSH, Redfish. Wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows. Nadawanie ról użytkownikom. Możliwość zarządzania minimum 200 serwerami z poziomu modułu zarządzającego pojedynczego serwera, na tym etapie dodatkowe licencje nie są wymagane. Możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem. Serwer umożliwia wykonanie aktualizacji oprogramowania do zarządzania serwerem, BIOS.

14.3 Możliwość zarządzania zdalnego poprzez darmową aplikację mobilną producenta serwera dostępną w AppStore dla systemów iOS. Aplikacja musi umożliwiać podłączenie do serwera przez sieć wi-fi lub przez port USB na froncie obudowy. Aplikacja musi umożliwiać:

14.3.1 sprawdzenie aktualnego poboru mocy przez zasilacze

14.3.2 sprawdzenie temperatury powietrza na wlocie do serwera

14.3.3 sprawdzenie modelu kontrolera RAID oraz utworzonych dysków fizycznych i logicznych

14.3.4 sprawdzenie ilości zainstalowanych modułów pamięci, pojemności, taktowania, numerów seryjnych i slotu w którym są zainstalowane

14.3.5 sprawdzenie zainstalowanych procesorów , taktowania zegara ilości rdzeni, wątków oraz pamięci Cache

14.3.6 wyświetlanie alarmów dot. pracy serwera z podziałem na kategorie według istotności

14.3.7 konfiguracje adresacji IP portu management port

14.3.8 włączenie oraz wyłączenie serwera

14.3.9 sprawdzenie wersji firmware

15. Certyfikaty i Deklaracje

15.1 Deklaracja zgodności UE (Certyfikat CE).

15.2 Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.

15.3 Serwer musi być zaprojektowany i produkowany zgodnie z normą ISO-9001 lub równoważną oraz zaprojektowany i produkowany zgodnie z normą ISO-14001 lub równoważną.

16. Wsparcie serwisowe

16.1 Urządzenie musi być wyprodukowane nie wcześniej niż w 2024 roku i pochodzić z legalnego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub partnera serwisowego na terenie RP.

16.2 Urządzenie musi zostać objęte gwarancją w trybie 9x5 NBD onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki.

16.3 Urządzenie przystosowane do napraw w miejscu instalacji.

16.4 Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:

16.4.1 możliwość pobierania najnowszego firmware.

16.4.2 dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń.

16.4.3 otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware.

**[MACIERZ DYSKOWA]**

1 szt. macierz dyskowa, protokoły blokowe i plikowe

Minimalne wymaganie dotyczące macierzy:

1. Obudowa

1.1 System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''

2. Pojemność:

2.1 System musi zostać dostarczony w konfiguracji zawierającej minimum:

2.1.1 12 dysków 3,8 TB SSD

2.2 System musi posiadać możliwość rozbudowy o kolejne dyski

2.3 System musi wspierać dyski:

2.3.1 SSD: 800GB do 7600GB

2.4 Budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby kopiowania/migrowania danych (zamawiający przez model wyższy rozumie inny model macierzy danego producenta z większą pamięcią cache oraz mocniejszymi procesorami).

2.5 Zamawiający dopuszcza rozwiązanie które nie pozwala na rozbudowę do wyższego modelu przy założeniu, że zostanie zaoferowany najwyższy model z rodziny z pamięcią Cache min 1TB na kontroler.

2.6 System musi mieć możliwość rozbudowy do 500 dysków w obrębie pary kontrolerów lub w obrębie klastra wielu kontrolerów (scale-out) w zależności od sposobu realizacji rozbudowy dla oferowanego rozwiązania.

2.7 W przypadku klastrowania kontrolerów macierzy, system musi działać pod kontrolą jednego systemu operacyjnego od jednego producenta, niedopuszczalne jest zestawienie systemu klastrowego poprzez wykorzystanie serwerów pośredniczących i oprogramowania dodatkowego.

2.8 Dla rozwiązań wykorzystujących klastrowanie (scale-out) musi być możliwość rozbudowy rozwiązania do co najmniej 12 kontrolerów w klastrze.

2.9 Rozwiązanie musi pozwalać na rozbudowę o dyski lub kontrolery wykonane w technologii NVMe do min 1120 dysków w technologii NVME. Zamawiający dopuszcza zaoferowanie rozwiązania, które nie posiada takiej możliwości w przypadku gdy całość zasobów zostanie dostarczona na dyskach flash/SSD.

3.Kontroler

3.1 Dwa kontrolery wyposażone w przynajmniej 32GB cache każdy.

3.2 Procesory macierzy powinny być wykonane w technologii wielordzeniowej z przynajmniej 12 rdzeniami na każdy kontroler dla procesorów X86. Dla innych rodzajów procesorów min 64 rdzenie.

3.3 W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub poprzez zrzut na pamięć nieulotną

3.4 Macierz musi pozwalać na poszerzenie pamięci Cache za pomocą dysków SSD do 6TB.

Interfejsy

4.1 Oferowana macierz musi posiadać minimum

4.1.1 4 porty 10GbE SFP+

4.1.2 4 porty 16Gb FC bez wkładek SFP

4.1.3 2 porty 1Gb do zarządzania

4.1.4 4 porty 12Gb SAS,

4.2 Macierz musi pozwalać na zamianę wkładek z 10GbE na 16Gb FC.

5.RAID

5.1 System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID

6. Kopie Migawkowe

6.1 Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/-5%

6.2 Zamawiający dopuszcza rozwiązanie, które ma wpływ na wydajność przy stosowaniu kopii migawkowych przy zapisie, przy założeniu zaoferowania całej pojemności na dyskach SSD/Flash/NVME.

7.Obsługiwane protokoły

7.1 Macierz musi obsługiwać jednocześnie protokoły FC, iSCSi, CIFS i NFS, S3 (macierz obiektowa) - jeśli wymagane są licencje zamawiający wymaga dostarczenia ich wraz z macierzą.

8. Inne wymagania

8.1 Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2019 i nowsze, Linux, Vmware, Unix

8.2 Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie

8.3 Macierz musi posiadać funkcjonalność priorytetyzacji zadań.

8.4 Macierz musi posiadać funkcjonalność kompresji danych w trybie in-line oraz off-line na każdym rodzaju danych.

8.5 Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych którą można stosować na macierzy/danych produkcyjnej dla wszystkich rodzajów danych. Macierz powinna mieć możliwość czynności odwrotnej tzn. Cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie. Jeżeli oferowane rozwiązanie nie posiada funkcjonalności deduplikacji danych, zamawiający wymaga dostarczenia 4-krotności przestrzeni wyspecyfikowanej.

8.6 Macierz musi posiadać funkcjonalność replikacji synchronicznej i asynchronicznej pomiędzy macierzami tego samego producenta. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikowania replikowanych danych lub dwukrotnego zwiększenia pojemności ze względu na rozważaną w przyszłości replikację całości zasobów. Macierz musi posiadać możliwość w ramach zaoferowanych licencji zaimplementowanie klastra geograficznego.

8.7 System musi posiadać specjalny moduł do zabezpieczenia przez atakiem Ransomware w szczególności:

8.7.1 musi informować administratora w przypadku niestandardowego zachowania systemu oraz danych

8.7.2 wykonywać prewencyjną kopię migawkową „snapshot” w przypadku zagrożenia atakiem ransomware

8.7.3 monitorować niestandardowe zachowanie użytkowników serwera plików

8.8 Macierz musi posiadać zaimplementowaną funkcjonalność WORM. Jeżeli rozwiązanie wymaga do tego licencji zamawiający wymaga jej dostarczenia.

8.9 W celach bezpieczeństwa macierz musi posiadać funkcjonalność wieloetapowej akceptacji wybranych operacji tj. operacje takie jak: Skasowanie LUN/Wolumeny, skasowanie Snapshotu, wyłączenie replikacji. System musi pozwalać by wykonanie w/w operacji było akceptowane przez przynajmniej dwóch administratorów w celu zwiększenia bezpieczeństwa i uniknięcia błędów ludzkich.

8.10 Macierz musi posiadać możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy.

8.11 Macierz musi posiadać funkcjonalność wykonania wirtualnych klonów, które nie wymagają kopiowania bloków danych.

8.12 Z macierzą zamawiający wymaga dostarczenia oprogramowania które pozwala na:

8.12.1 monitoring wykorzystania przestrzeni na macierzy

8.12.2 monitoring grup RAIDowych

8.12.3 monitoring wykonywanych backupów/replikacji danych między macierzami

8.12.4 monitoring wydajności macierzy

8.12.5 analizę i diagnozę spadku wydajności

8.13 Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność macierzy.

8.14 Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy

8.15 Producent musi dostarczyć usługę w postaci portalu WWW lub dodatkowego oprogramowania umożliwiającą następujące funkcjonalności:

8.15.1 Narzędzie do tworzenia procedury aktualizacji oprogramowania macierzowego.

- procedura musi opierać się na aktualnych danych pochodzących z macierzy oraz najlepszych praktykach producenta.

- procedura musi uwzględniać systemy zależne np, macierze replikujące

- procedura musi umożliwiać generowanie planu cofnięcia aktualizacji.

8.15.2 Wyświetlanie statystyk dotyczących wydajności, utylizacji, oszczędności uzyskanych dzięki funkcjonalnościom macierzy.

8.15.3 Wyświetlanie konfiguracji macierzy oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji.

8.16 Portal lub oprogramowanie może pochodzić od innego producenta niż producent macierzy, z tym że zostanie dostarczona odpowiednia licencja do maksymalnej pojemności macierzy.

8.17 Zamawiający wymaga by wszystkie funkcjonalności działały wspólnie tj. włączenie jednej funkcjonalności nie eliminowało innej.

9. Gwarancja i serwis

9.1 serwis a z 2-godzinnym czasem odpowiedzi na awarie krytyczne i dostawą elementów w na następny dzień roboczy

9.2 Dostarczony system musi posiadać również 2 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.

**[SERWEROWE SYSTEMY OPERACYJNE]**

**Zamawiający oczekuje dostawy dwóch systemów.**

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

Przedmiot zamówienia powinien odznaczać się następującymi cechami:

1. Przedmiotem zamówienia jest system do budowy infrastruktury wirtualnej, złożonej z przynajmniej 3 serwerów (po 2 CPU 16cores) wraz z konsolą zarządzającą, mechanizmem wysokiej dostępności HA, bez ograniczenia liczby maszyn wirtualnych.

2. Warstwa wirtualizacji musi być instalowana bezpośrednio na sprzęcie fizycznym bez potrzeby instalowania dodatkowego systemu operacyjnego.

3. Oprogramowanie do wirtualizacji musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i musi się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.

4. Oprogramowanie do wirtualizacji musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych, niż fizyczne zasoby RAM serwera, w celu osiągniecia konsolidacji.

5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 1TB pamięci operacyjnej.

6. Oprogramowanie do wirtualizacji musi być niezależne od producenta platformy sprzętowej.

7. Oprogramowanie do wirtualizacji musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi, zasobami i warstwą sieciową na wszystkich hostach. Konsola powinna być możliwa do zainstalowania na niezależnej maszynie fizycznej pracującej pod kontrolą systemu operacyjnego BSD, Linux lub Windows.

8. Oprogramowanie do wirtualizacji musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.

9. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich sprawnego odtwarzania.

10. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.

11. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.

12. Oprogramowanie do wirtualizacji musi umożliwiać udostepnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane.

13. Oprogramowanie do wirtualizacji musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.

14. Oprogramowanie do wirtualizacji musi zapewniać funkcjonalność HA zapewniającą automatyczną migrację maszyn wirtualnych pomiędzy serwerami bez przerywania pracy użytkowników lub ograniczenia dostępności usługi przy awarii jednego z hostów.

15. W ramach usługi wsparcia technicznego dla Oprogramowania, w ramach uiszczonego przez Zamawiającego na rzecz Wykonawcy wynagrodzenia, Zamawiającemu przysługuje, przez okres co najmniej do końca czerwca 2026 r.:

15.1 prawo do korzystania, bez jakichkolwiek dodatkowych opłat z wydawanych przez producenta Oprogramowania najnowszych jego wersji, aktualizacji Oprogramowania, poprawek do Oprogramowania;

15.2 zdalny dostęp elektroniczny przez całą dobę i wszystkie dni w roku (7X24) do Centrum Pomocy Technicznej Oprogramowania, z czasem podjęcia naprawy nie przekraczającym jednego dnia roboczego od momentu zgłoszenia problemu;

15.3 zdalny dostęp elektroniczny do bazy wiedzy, dokumentacji, biuletynów i informacji na temat Oprogramowania.

15.4 Szczegółowe warunki wsparcia technicznego dla Oprogramowania, o którym mowa powyżej regulować powinny umowy licencyjne lub inne stosowne umowy lub warunki wydane lub zaakceptowane przez producenta Oprogramowania, przy czym umowy takie, ani warunki nie mogą ograniczać wskazanych powyżej wymagań, ani stać z nimi w sprzeczności.

**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 40 kW**

Minimalne wymaganie dotyczące jednej sztuki agregatu.

1. Rodzaj agregatu: Stacjonarny

2. Gwarancja: minimum 24 miesiące

3. Moc agregatu (znamoniowa/maksymalna 15 min): 40 kW

4. Stopień sprężania: 19:01

5. System zasysania: Naturalny

6. Typ agregatu Trójfazowy

7. Sprawność cos Φ: 0.8

8. Obudowa

8.1 Typ zabudowy: Zabudowane - Wyciszone

8.2 Możliwość odprowadzenia spalin poza obiekt: Tak

8.3 Zabudowa odporna na opady atmosferyczne: Tak

8.4 Poziom ciśnienia akustycznego LPA 85dB (pomiar - 5m, otwarta przestrzeń)

8.5 Ilość gniazd trójfazowych: 1 sztuka (63A 5-bolcowe)

8.6 Ilość gniazd jednofazowych: 2 sztuki (16A)

8.7 Ilość gniazd pozostałych: Brak

8.8 Pojemność zbiornika paliwa: 135 litrów

8.9 Czas pracy na pełnym zbiorniku (Średni): 20 godzin

9. Cechy fizyczne

9.1 Długość: max. 220 cm

9.2 Szerokość: max. 95 cm

9.3 Wysokość: max. 123 cm

9.4 Waga netto: max. 1070 kg

9.5 Waga brutto: max. 1240 kg

10. Funkcje

10.1 Automatyczny start (SZR): Tak - wyposażony

10.2 Stabilizator napięcia (AVR): Tak - 2%, Stamford SX460

10.3 Rodzaj rozruchu: Elektryczny Automatyczny

10.4 Zabezpieczenie przeciążeniowe termiczne: Tak

10.5 Świece żarowe: Tak

10.6 Podgrzewanie miski olejowej: Tak

10.7 Podgrzewanie cieczy chłodzącej: Tak

10.8 Wskaźnik poziomu paliwa: Tak

10.9 Akumulator: 2 sztuki 40Ah

10.10 Licznik motogodzin: Tak

10.11 Amperomierz: Tak

10.12 Woltomierz: Tak

10.13 Logika PLC: Wbudowana logika PLC i edytor PLC

10.14 Rozszerzenia modułu CAN: Tak

10.15 Dodatkowe wyjścia: Dwa gniazda na moduły wtykowe do połączeń 4G, Ethernet, RS232/485 oraz dodatkowe wejścia i wyjścia binarne

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

Zasilacz UPS 3-fazowy o mocy 30 000 VA

1. Minimalne wymagania techniczne dla jednostki UPS

1.1 Moc znamionowa jednostki nie mniej niż 30 kVA / 30 kW

1.2 Obudowa typu szafa/wieża

1.3 Technologia Podwójnej konwersji (online)

1.4 Temperatura pracy 0 - 40 °C

1.5 Wilgotność względna podczas pracy 0 - 95 %

1.6 Wysokość pracy n.p.m. 1000m

1.7 Wymiary (wys. x szer. x dł.): 770 x 250 x 800 mm

1.8 Sprawność online ? 94,7% przy pełnym obciążeniu

1.9 Klasa ochrony IP 20

1.10 Maksymalny poziom dźwięku: 63 dBA

1,11 Waga maksymalna: 60 kg

2. Parametry wejściowe

2.1 Nominalne napięcie wejściowe 400V 3 fazy

2.2 Częstotliwość sieciowa 45–65 Hz

2.3 Typ gniazda wejściowego: zaciski

2.4 Zakres napięcia wejściowego 304...477 V

2.5 Zniekształcenia natężenia wejściowego THDi: <3%

3. Parametry wyjściowe

3.1 Napięcie wyjściowe 400VAC

3.2 Zniekształcenia napięcia wyjściowego THDu <3% dla liniowego obciążenia

3.3 Częstotliwość na wyjściu (synchronicznie z siecią) 50/60Hz

3.4 Przeciążenia 10 minut przy 125% i 60 sekund przy 150%

3.5 Współczynnik szczytu 3:1

3.6 Złącza/gniazda wyjściowe: zaciski

3.6 Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)

4. Akumulatory i czas podtrzymania

4.1 Systemem baterii zewnętrznych - możliwość dokupienia

4.2 Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów

5. Komunikacja i zarządzanie

5.1 Gniazdo do montażu karty WEB/SNMP

5.2 RS232, RS485, SNMP, Dry contacts, USB

5.3 Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD

5.4 Alarm dźwiękowy Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia

5.5 Awaryjny wyłącznik zasilania (EPO): Tak

5.6 Darmowe oprogramowanie do zamykania systemów operacyjnych

6. Certyfikaty, zgodności oraz gwarancja

6.1 CE, EAC, RCM

6.2 gwarancja naprawy lub wymiany w trybie on-site na okres minimum do końca czerwca 2026 r.

11. Inne wymagania:

11.1 UPS i agregat w ramach rozruchu ma być podłączony, zintegrowany z siecią urzędu, wyłącznikiem p. poż. (wykonanie połączeń kablowych na styku sieci budynku urzędu i dostarczonych urządzeń w tym CAN)

11.2 UPS montowany w piwnicy budynku – wymagane posadowienie na stelażu o wysokości 0,25m-0,5m

11.3 Wymagane właściwe oznakowanie miejsca instalacji UPS w zakresie bezpieczeństwa

**[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.