



Cyberbezpieczny Samorząd



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

ZAŁĄCZNIK NR 8 – Wzór umowy

nr umowy:/WO/24

zawarta w dniu r. w Krobi (zwana dalej „Umową”)

pomiędzy:

Gminą Krobia, z siedzibą w Krobi 63-840 ul. Rynek 1,

reprezentowaną przez:

Łukasza Kubiaka - Burmistrza Krobi,

przy kontrasygnacie Skarbnika Gminy Damiana Walczaka

zwaną dalej „Zamawiającym”,

a

.....
.....

zwaną/ym dalej „Wykonawcą”,

łącznie zwanymi „Stronami”,

o następującej treści:

§ 1 Przedmiot umowy

1. Zamawiający powierza do wykonania, a Wykonawca zobowiązuje się do realizacji zadania pod nazwą: Poprawa Cyberbezpieczeństwa w Gminie Krobia poprzez dostawę i wdrożenie,

systemu przechowywania danych, oprogramowanie kopii bezpieczeństwa, klastra firewall wraz ze szkoleniem technicznym oraz przełączników sieciowych.

2. Szczegółowy przedmiot zamówienia znajduje się w załączniku nr 1 do Umowy.

§ 2 **Termin realizacji**

1. Wykonawca zobowiązuje się wykonać przedmiot umowy **w terminie:**dni od podpisania umowy.

2. Termin zakończenia zadania, o którym mowa w ust. 1 uważa się za zachowany, jeśli w tym terminie Wykonawca dokonana pisemnego zgłoszenia Zamawiającemu zakończenia zadania.

§ 3 **Wynagrodzenie**

1. Za wykonanie przedmiotu umowy określonego w § 1 niniejszej umowy, Strony ustalają wynagrodzenie ryczałtowe w wysokości:

..... zł **netto** (słownie:
.....) powiększone o podatek VAT, co
daje kwotę **brutto**zł (słownie:
.....).

2. Płatność za wykonanie przedmiotu Umowy, nastąpi w ciągu **do 14 dni** od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury.

3. Zamawiający nie dopuszcza fakturowania częściowego.

4. Zamawiający nie przewiduje płatności w 2024 r.

5. Podstawą wystawienia faktury będzie podpisany ze strony Zamawiającego protokół zdawczo-odbiorczy podpisany przez strony umowy.

6. Wynagrodzenie ryczałtowe, o którym mowa w ust. 1 obejmuje wszystkie koszty związane z realizacją przedmiotu umowy, w tym ryzyko Wykonawcy z tytułu oszacowania wszelkich kosztów związanych z realizacją przedmiotu umowy, a także oddziaływania innych czynników mających lub mogących mieć wpływ na koszty.

Niedoszacowanie, pominięcie oraz brak rozpoznania zakresu przedmiotu umowy nie może być podstawą do żądania zmiany wynagrodzenia ryczałtowego określonego w ust. 1 niniejszego paragrafu.

7. Zamiast faktury w formie papierowej lub elektronicznej wystawionej na Gminę Krobia Wykonawca ma możliwość (ale nie jest obowiązany) wystawiania i wysyłania ustrukturyzowanych faktur elektronicznych do Gminy Krobia za pośrednictwem platformy elektronicznego fakturowania <https://brokerpefexpert.efaktura.gov.pl> na adres PEF: NIP

6961749038 – w przypadku wystawiania faktur elektronicznych na wskazany adres PEF Nabywcą/Odbiorcą towaru/usługi jest **Gmina Krobia, ul. Rynek 1, 63-840 Krobia, NIP: 6961749038.**

8. Zamawiający jest obowiązany do odbierania od Wykonawcy ustrukturyzowanych faktur elektronicznych przesłanych za pośrednictwem platformy na adres PEF wskazany przez Zamawiającego. Przepisu art. 106n ust. 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług nie stosuje się.

9. Zgodnie z art. 4 ust. 4 ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz.U. z 2020 r. poz. 1666 ze zm.), Zamawiający i Wykonawca mogą wysyłać i odbierać inne ustrukturyzowane dokumenty elektroniczne za pośrednictwem platformy, jeżeli druga strona wyrazi na to zgodę.

§ 4 Odbiór przedmiotu zamówienia

1. Wykonawca dostarczy przedmiot zamówienia do Urzędu Miejskiego w Krobi.
2. Zamawiający dokona odbioru przedmiotu umowy w przeciągu 14 dni od zgłoszenia gotowości do odbioru na podstawie zgodności z Opisem Przedmiotu Zamówienia w formie uzgodnionej z wykonawcą.
2. Dokumentami potwierdzającymi przyjęcie przez Zamawiającego przedmiotu zamówienia jest protokół zdawczo – odbiorczy podpisany przez strony umowy.
3. Braki ilościowe lub wady jakościowe stwierdzone w przedmiocie umowy Zamawiający reklamuje w ciągu 7 dni roboczych od ich stwierdzenia. Wykonawca zobowiązuje się na własny koszt do uzupełnienia braków lub usunięcia wad niezwłocznie, nie później jednak niż w terminie 7 dni roboczych, licząc od daty otrzymania wezwania.

§ 5 Podwykonawcy

1. Wykonawca może zrealizować usługi wskazane w ofercie korzystając z pomocy podwykonawców i dalszych podwykonawców na zasadach określonych w Umowie oraz w ustawie Pzp.
2. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.

3. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonania tego zamówienia.
4. Umowa o podwykonawstwo nie może zawierać postanowień kształtujących prawa i obowiązki podwykonawcy w zakresie kar umownych oraz postanowień dotyczących warunków wypłaty wynagrodzenia, w sposób dla niego mniej korzystny niż prawa i obowiązki wykonawcy, ukształtowane postanowieniami umowy zawartej między zamawiającym a wykonawcą.

§ 6

Gwarancja i rękojmia

1. Wykonawca na dostarczony sprzęt udziela gwarancji:
 - a) miesięcy na sprzęt wymieniony w pkt. 1, 2, 3 załącznika nr 1 do Umowy
 - b) 24 miesiące na sprzęt wymieniony w pkt. 6,7 załącznika nr 1 do Umowy
 - c) 12 miesięcy na sprzęt wymieniony pkt. 5 załącznika nr 1 do Umowy
2. Jeżeli w okresie gwarancji zostaną stwierdzone wady, Wykonawca zrealizuje swoje zobowiązania wynikające z udzielonej gwarancji w terminie wyznaczonym przez Zamawiającego.
3. Termin na usunięcie wady nie może być dłuższy niż 21 dni od daty pisemnego powiadomienia Wykonawcy o jej wystąpieniu, chyba, że Strony w poszczególnym przypadku uzgodnią inaczej. Przy uzgadnianiu lub wyznaczaniu terminu do usuwania wad Strony zobowiązane są uwzględnić charakter wady, wpływ na funkcjonowanie sprzętu, rzeczywiste możliwości Wykonawcy wynikające z uwarunkowań technicznych.
4. Wykonawca udziela rękojmi na okres tożsamy z okresem gwarancji. Termin rękojmi rozpoczyna swój bieg od daty podpisania bez zastrzeżeń protokołu zdawczo-odbiorczego obejmującego potwierdzenie prawidłowego wykonania przedmiotu umowy.

§ 7

Kary umowne

1. Wynagrodzenie umowne dla ustalenia kar umownych – jest to wynagrodzenie ryczałtowe (brutto) określone w niniejszej umowie.
2. Wykonawca zapłaci Zamawiającemu kary umowne w następujących przypadkach:
 - 1) w przypadku odstąpienia przez Zamawiającego lub Wykonawcę od niniejszej Umowy lub rozwiązania Umowy z powodu okoliczności leżących po stronie Wykonawcy, Zamawiającemu przysługuje prawo żądania kary umownej w wysokości 3% wynagrodzenia umownego,

- 2) w przypadku odstąpienia przez Wykonawcę lub Zamawiającego od niniejszej Umowy lub rozwiązania Umowy z powodu okoliczności leżących po stronie Zamawiającego, Wykonawcy przysługuje prawo żądania kary umownej w wysokości 2% wynagrodzenia umownego,
 - 3) za zwłokę w zakończeniu wykonania przedmiotu umowy – w wysokości 0,1 % wynagrodzenia umownego za każdy dzień zwłoki,
 - 4) za zwłokę w usuwaniu wad stwierdzonych w okresie rękojmi lub gwarancji w wysokości 0,1 % wartości wynagrodzenia umownego brutto Wykonawcy, za każdy rozpoczęty dzień zwłoki w stosunku do terminów przyjętych w Umowie lub uzgodnionych przez strony.
3. Strony zastrzegają sobie prawo do odszkodowania na zasadach ogólnych, o ile wartość faktycznie poniesionych szkód przekroczy wysokość kar umownych.
4. Łączna maksymalna wysokość kar umownych, których mogą dochodzić strony nie może przekraczać 50% wynagrodzenia ryczałtowego (brutto).

§ 8

Zmiana treści umowy

1. Kierując się zapisami art. 455 ust. 1 pkt 1 ustawy Prawo zamówień publicznych, Zamawiający dopuszcza dokonanie zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy w następujących przypadkach:

- a) zmiany rozwiązań ze względu na postęp techniczny lub technologiczny (np. wycofanie z obrotu urządzeń lub podzespołów), zmiana nie może spowodować podwyższenia ceny oraz obniżenia parametrów technicznych, jakościowych i innych wynikających z oferty (opisu przedmiotu zamówienia / opisu oferowanego towaru), na podstawie której był dokonany wybór Wykonawcy,
- b) gdy nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację umowy, w tym: zmiana stawki podatku od towarów i usług na asortyment stanowiący przedmiot umowy oraz podatku akcyzowego – w takim przypadku obniżenie lub podwyższenie wynagrodzenia jest możliwe w wysokości odpowiadającej zmianie podatku od towarów i usług oraz podatku akcyzowego,
- c) zmiany terminu realizacji zamówienia z powodu działania siły wyższej, za które uważa się zdarzenia o charakterze nadzwyczajnym, występujące po zawarciu umowy, a których Strony nie były w stanie przewidzieć w momencie jej zawarcia i których zaistnienie lub skutki uniemożliwiają wykonanie przedmiotu umowy w terminie, przy czym ewentualne przedłużenie terminu realizacji zamówienia nastąpi o liczbę dni, odpowiadającą okresowi występowania siły

wyższej - podstawą dokonania zmian, o których mowa wyżej będzie wystąpienie opisanych okoliczności uzasadniających wstrzymanie dostaw, z określeniem okresu wpływającego na zmianę terminu i sporządzenie protokołu konieczności – zatwierdzonego przez Zamawiającego

- d) zaistnienie okoliczności leżących po stronie Zamawiającego, w szczególności spowodowanych sytuacją finansową, zdolnościami płatniczymi lub warunkami organizacyjnymi; zmianie może ulec termin realizacji zamówienia, zmiana zostanie wprowadzona stosownie do pisma Zamawiającego określającego te okoliczności.

2. Wykonawca wnioskujący o zmianę umowy, przedkłada Zamawiającemu pisemne uzasadnienie konieczności wprowadzenia zmian do umowy wraz z niezbędnymi dowodami.
3. Wszelkie zmiany i uzupełnienia treści niniejszej umowy wymagają aneksu sporządzonego z zachowaniem formy pisemnej pod rygorem nieważności.
4. Zmiany mogą być dokonane tylko, jeżeli jest to niezbędne dla prawidłowego wykonania przedmiotu umowy.

§ 9 Odstąpienie od umowy

1. Zamawiający zastrzega prawo odstąpienia od umowy z Wykonawcą ze skutkiem natychmiastowym w przypadku rażących zaniedbań w wykonywaniu obowiązków Wykonawcy przewidzianych w umowie bądź wykonywania prac niezgodnie z umową.
2. Jeżeli Wykonawca będzie realizował przedmiot umowy wadliwie albo sprzecznie z umową, Zamawiający może wezwać go do zmiany sposobu wykonywania umowy i wyznaczyć mu w tym celu odpowiedni termin. Po bezskutecznym upływie wyznaczonego terminu Zamawiający może od umowy odstąpić, powierzyć poprawienie lub dalsze wykonanie przedmiotu umowy innemu podmiotowi na koszt Wykonawcy.

§ 10 Siła Wyższa

1. Żadna ze Stron Umowy nie będzie odpowiedzialna za niewykonanie lub nienależycie wykonanie zobowiązań wynikających z umowy, spowodowane przez okoliczności traktowane jako siła wyższa.
2. Siła wyższa oznacza zdarzenie zewnętrzne, nagłe, nieprzewidywalne i niezależne od woli Stron, uniemożliwiające wykonanie umowy w całości lub w części, na stałe lub pewien czas, któremu nie można zapobiec ani przeciwdziałać przy zachowaniu należytej staranności Stron. W szczególności strony traktują stan epidemii jako siłę wyższą.

3. W przypadku zaistnienia siły wyższej, Strona której taka okoliczność uniemożliwia lub utrudnia prawidłowe wywiązanie się z jej zobowiązań, powiadomi drugą stronę o takich okolicznościach i ich przyczynie.

§ 11

Postanowienia końcowe

1. Wykonawca nie może bez zgody Zamawiającego wyrażonej na piśmie pod rygorem nieważności, przenieść praw i obowiązków wynikających z Umowy na inny podmiot, w szczególności nie może dokonać cesji przysługujących mu wobec Zamawiającego wierzytelności.

2. Ewentualne spory cywilnoprawne wynikłe z niniejszej umowy Strony zobowiązują się poddać w sprawach, w których zawarcie ugody jest dopuszczalne, mediacjom lub innemu polubownemu rozwiązywaniu sporu przed Sądem Polubownym przy Prokuraturii Generalnej Rzeczypospolitej Polskiej, wybranym mediatorem albo osobą prowadzącą inne polubowne rozwiązanie sporu. W razie braku możliwości osiągnięcia porozumienia spory cywilnoprawne wynikłe w związku z realizacją niniejszej umowy, rozstrzygać będzie sąd właściwy dla siedziby Zamawiającego.

3. W okresie, w którym mogą być realizowane roszczenia z niniejszej Umowy, strony są zobowiązane informować się nawzajem na piśmie o każdej zmianie adresu swojego zamieszkania lub siedziby. W razie zaniedbania tego obowiązku korespondencję wysłaną na uprzednio wskazany adres listem poleconym za potwierdzeniem odbioru i nieodebraną, uważa się za doręczoną.

4. W sprawach nie unormowanych niniejszą umową mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r. — Kodeks cywilny (t. j. Dz. U. 2024 r. poz. 1061 ze zm.), ustawy z dnia 11 września 2019 r. — Prawo zamówień publicznych (t. j. Dz. U. 2024 poz. 1320) wraz z przepisami wykonawczymi.

5. Niniejszą Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron

ZAMAWIAJĄCY :

WYKONAWCA:

KONTRASYGNA TA SKARBNIKA:

Poprawa Cyberbezpieczeństwa w Gminie Krobia poprzez dostawę i wdrożenie, systemu przechowywania danych, oprogramowanie kopii bezpieczeństwa, klastra firewall wraz ze szkoleniem technicznym oraz przełączników sieciowych

Zamówienie realizowane w ramach projektu grantowego Cyberbezpieczna Gmina Krobia Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1329/ FERC.02.02-CS.01-001/23/2024 realizowanego w ramach konkursu grantowego „Cyberbezpieczny Samorząd”.

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu

FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC)

Opis Przedmiotu zamówienia:

1. System do przechowywania danych :

1.1. Macierz dyskowa – 1 sztuka wraz z wdrożeniem.

Wdrożenie obejmuje:

- Instalację dostarczonej macierzy w szafie rack
- Podłączenie macierzy do infrastruktury LAN Zamawiającego
- Konfigurację sieci SAN (iSCSI)
- Udostępnienie wolumenów do dostarczonych serwerów.
- Sprawdzenie poprawności działania, obejmujące m. in. symulację awarii pojedynczego dysku oraz pojedynczego kontrolera.

LP.	Funkcjonalność
1.	Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowana macierz nie może przekroczyć rozmiaru 2U. Obudowa musi umożliwiać instalację min. 24 dysków.
2.	Oferowane urządzenie musi być przystosowane do zasilania z sieci AC oraz wyposażone w kable zasilające PDU. Macierz musi być wyposażona

	w zdublowany, redundantny system zasilania, umożliwiający prawidłową, nieprzerwaną pracę urządzenia w przypadku awarii dowolnego pojedynczego źródła zasilania.
3.	Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Architektura symmetric active-active. Praca kontrolerów w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek i portów kontrolerów bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery nie mogą pracować w trybie active-passive.
4.	<p>Macierz w oferowanej konfiguracji w teście wydajnościowym osiągnie min. 100 000 IOPS przy następujących parametrach:</p> <ul style="list-style-type: none"> • Zapełnienie macierzy – min. 75% fizycznej pojemności, • Protokół: iSCSI, • Porty: 10Gb, • Read 80% - blok 8k, • Write 20% - blok 8k, • 100% Random • Read Hit Ratio – 0% • Write Hit Ratio – 0% • Latency – max. 1ms • RAID 6 <p>Zamawiający ma prawo przeprowadzić test po dostawie macierzy aby sprawdzić czy dostarczone rozwiązanie osiąga deklarowane parametry wydajnościowe.</p>
5.	Fizyczna przestrzeń dyskowa zbudowana za pomocą dysków SSD SAS. Przestrzeń użytkowa po zbudowaniu RAID 6 z 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności 1 dysku, musi wynosić min 16 TB. Ze względów wydajnościowych oraz niezawodnościowych rozmiar pojedynczego dysku nie może być większy niż 4 TB. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń spare i dostępna dla hostów bez uwzględnienia mechanizmów kompresji, czy deduplikacji.

	Dyski muszą być wyposażone w podwójne interfejsy. Niedopuszczalne są dyski SSD zbudowane w oparciu o technologię QLC.
6.	Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
7.	Rozbudowa oferowanej macierzy, do co najmniej 98 dysków SSD SAS, bez wymiany kontrolerów macierzowych oraz bez rozbudowy o dodatkowe kontrolery, tylko poprzez dodawanie półek i dysków SSD SAS.
8.	Co najmniej 128GB pamięci cache na całą macierz (dwa kontrolery). Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć.
9.	Razem kontrolery muszą udostępnić minimum 12 portów 10Gb Eth. Wymagana możliwość rozbudowy o dodatkowe 8 portów 10Gb Eth lub 8 portów 16G FC bez konieczności wymiany lub zakupu nowych kontrolerów i klastrowania z kontrolerami oferowanymi w tym postępowaniu. Wszystkie moduły muszą posiadać wkładki optyczne SFP+. Macierz musi posiadać wbudowane min. 4 porty SAS 12Gb/s do podłączenia półek dyskowych.
10.	Wymagane wsparcie dla protokołów iSCSI. Wsparcie dla protokołu FC po rozbudowie macierzy o interfejsy FC.
11.	Kontrolery wyposażone w funkcjonalność konfiguracji poziomego RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych.
12.	Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Macierz musi wspierać nie mniej niż 1024 LUNów. Wymagana możliwość tworzenia grup wolumenów. Max. liczba LUNów w grupie wolumenów nie może być mniejsza niż 100.
13.	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego

	<p>interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy w tym monitorowanie wydajności obiektów takich jak:</p> <ul style="list-style-type: none"> • cała macierz • kontrolery • porty front-end • dyski • LUNy • hosty <p>Pod kątem parametrów takich jak:</p> <ul style="list-style-type: none"> • operacje wejścia/wyjścia IOPS • przepustowość (KB/s lub MB/s) • czas odpowiedzi (latency) <p>Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS.</p> <p>Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Wymagana możliwość konfigurowania zasobów macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.</p>
14.	<p>Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych. Snapshoty muszą być wykonywane w technologii ROW (Redirect On Write). Macierz musi obsługiwać min 2000 snapshotów.</p> <p>Wymagane wsparcie dla snapshotów kaskadowych.</p> <p>Wymagana możliwość tworzenia harmonogramu wykonywania snapshotów oraz zabezpieczenia migawek przed modyfikacją lub usunięciem pod kątem szybkiego przywrócenia danych w przypadku ataku ransomware.</p> <p>Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model macierzy.</p> <p>Tworzenie na żądanie kopii danych typu klon w ramach macierzy za pomocą</p>

	wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z wolumenu źródłowego na docelowy oraz resynchronizację danych z wolumenu docelowego na źródłowy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
15.	Macierz musi wspierać funkcjonalności deduplikacji i kompresji danych w trybie in-line (w locie). Musi być możliwe włączenie deduplikacji i kompresji per wolumen (LUN). Musi istnieć możliwość wyłączenia tych funkcjonalności na wybranych wolumenach (LUN). Dostarczenie licencji na tę funkcjonalność jest wymagane na tym etapie postępowania.
16.	Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie asynchronicznym oraz synchronicznym przy wykorzystaniu portów FC lub IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
17.	Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra klasy "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych po protokole FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Dopuszczalne jest zastosowanie tzw arbitra (serwer quorum). Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
18.	Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s. Musi istnieć

	możliwość określenia polityk QoS na poziomie wolumenów. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
19.	Macierz musi oferować wsparcie dla zachowania integralności danych na całej ścieżce transferu (ang. End-to-End) zgodnego ze standardem/specyfikacją T10 PI.
20.	Wsparcie, dla co najmniej Microsoft Server Windows 2016/2019/2022, VMware 7.x/8.x, Linux RedHat 7.x/8.x, CentOS 7.x/8.x
21.	<p>Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączenia.</p> <p>Macierz musi umożliwiać zdalne zarządzanie. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.</p> <p>Wymagana gwarancja 3 lata w trybie 9x5 NBD.</p>

1.2. Serwer – 2 sztuki wraz z wdrożeniem.

Wdrożenie obejmuje:

- Montaż serwerów w szafie rack.
- Instalację środowiska wirtualizującego (VMware lub równoważne)
- Konfigurację sieci w środowisku VMware lub równoważnym
- Podłączenie współdzielonych zasobów dyskowych udostępnionych z dostarczonej macierzy dyskowej.
- Konfigurację klastra HA.
- Sprawdzenie poprawności działania klastra HA.
- Migrację maszyn wirtualnych oraz fizycznych wskazanych przez Zamawiającego do zainstalowanego środowiska wirtualnego.

LP.	Funkcjonalność
1.	<p>Obudowa:</p> <ul style="list-style-type: none"> a. Typu RACK, wysokość maksymalnie 1U b. Szyny umożliwiające wysunięcie serwera z szafy wraz z ramieniem

	<p>porządkującym kable z tyłu obudowy</p> <p>c. Możliwość zainstalowania 8 dysków twardych hot-plug 2,5"</p> <p>d. Zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych</p> <p>e. Zainstalowane 2 dyski 2,5" SSD SATA 960GB hot-plug skonfigurowane w RAID1</p>
2.	<p>Płyta główna:</p> <p>a. Jednoprocessorowa</p> <p>b. Wyprodukowana i zaprojektowana przez producenta serwera</p> <p>c. Możliwość instalacji procesorów 128-rdzeniowych</p> <p>d. Zainstalowany moduł TPM 2.0</p> <p>e. Minimum 3 fizyczne złącza PCI Express generacji 5 o prędkości x16</p> <p>f. Minimum 24 gniazda pamięci RAM</p> <p>g. Obsługa minimum 6 TB pamięci RAM DDR5</p> <p>h. Możliwość instalacji 2 dysków M.2 na płycie głównej</p>
3.	<p>Procesor:</p> <p>a. Zainstalowany jeden procesor 16-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem</p> <p>b. Minimum 178 punktów w teście SPECrate@2017_int_base, dostępnym na stronie www.spec.org dla proponowanego serwera</p> <p>c. Taktowanie bazowe minimum 3.0 GHz</p> <p>d. Minimum 64 MB pamięci podręcznej L3</p>
4.	<p>Pamięć RAM:</p> <p>a. Minimum 192 GB pamięci RAM</p> <p>b. DDR5 RDIMM 4800 MT/s</p> <p>c. Pamięci obsadzone w sposób gwarantujący najwyższą możliwość wydajność</p> <p>d. Możliwość podwojenia ilości pamięci bez konieczności wymiany zainstalowanych modułów</p>
5.	<p>Kontrolery LAN:</p> <p>a. Dwie dwuportowe karty 10Gbit SFP+ nie zajmujące żadnego z dostępnych slotów PCI Express</p>

	<p>b. Możliwość zamiany kart 10Gbit SFP+ na dwie dwuportowe karty 100Gbit QSFP28 bez konieczności zajmowania slotów PCIe</p>
6.	<p>Kontrolery I/O:</p> <p>a. Kontroler SAS RAID dla dysków wewnętrznych, obsługujący poziomy RAID: 0,1,10</p>
7.	<p>Porty</p> <p>a. Zintegrowana karta graficzna ze złączem VGA z tyłu i z przodu serwera</p> <p>b. Minimum 2 porty USB 3.2 dostępne z tyłu serwera</p> <p>c. Minimum 2 porty USB 3.2 na panelu przednim</p> <p>d. Możliwość zainstalowania portu szeregowego (RS-232-C), możliwość wykorzystania portu szeregowego do zarządzania serwerem</p> <p>e. Liczba dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących złącza PCI Express i/lub USB serwera</p>
8.	<p>Zasilanie, chłodzenie:</p> <p>a. Redundantne zasilacze hot-plug o sprawności 96% (tzw. klasa Titanium) o mocy 900W</p> <p>b. Redundantne wentylatory hot-plug</p>
9.	<p>Zarządzanie</p> <p>a. Wbudowane diody informacyjne lub wyświetlacz informujący o stanie serwera - system przewidywania, rozpoznawania awarii</p> <p>b. informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:</p> <ul style="list-style-type: none"> • karty rozszerzeń zainstalowanej w dowolnym slotcie PCI Express • procesory CPU • pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM • wbudowany na płycie głównej nośnik pamięci M.2 SSD • status karty zarządzającej serwerem

	<ul style="list-style-type: none"> • wentylatory • bateria podtrzymująca ustawienia BIOS płyty głównej • zasilacze • system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym) <p>c. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:</p> <ul style="list-style-type: none"> • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie w tym zdalny restart serwera • Dedykowana karta LAN 1 Gb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym • Dostęp poprzez: przeglądarkę WWW, SSH • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Obsługa VLAN • Wsparcie dla protokołu SSDP • Obsługa protokołów TLS 1.3, SSL v3 • Obsługa protokołu LDAP • Synchronizacja czasu poprzez protokół NTP • Możliwość wykonywania kopii bezpieczeństwa ustawień bios serwera oraz ustawień karty zarządzającej <p>d. Oprogramowanie zarządzające i diagnostyczne wyprodukowane</p>
--	---

	<p>przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna)</p> <p>e. Dedykowana pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN</p> <p>f. Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej</p>
10.	<p>Wspierane systemy operacyjne:</p> <p>a. Microsoft Windows Server 2022</p> <p>b. VMWare vSphere 7, 8</p> <p>c. Suse Linux Enterprise Server 15</p> <p>d. Red Hat Enterprise Linux 9, 8</p> <p>e. Oracle Linux 9, 8</p>
11.	<p>Gwarancja</p> <p>a. 3 lata gwarancji producenta serwera w trybie onsite z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis</p> <p>b. Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu</p> <p>c. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych</p> <p>d. Bezpłatna dostępność poprawek i aktualizacji</p>

	<p>BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniony w ofercie</p> <p>e. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.</p>
12.	<p>Dokumentacja, inne:</p> <p>a. Elementy, z których zbudowany jest serwer muszą być produktami producenta serwera lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta</p> <p>b. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta</p> <p>c. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera</p> <p>d. W czasie obowiązywania gwarancji, możliwość sprawdzenia, po podaniu na infolinii numeru seryjnego urządzenia, pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typu udzielonej gwarancji</p> <p>e. Zgodność z normami: CB, RoHS, WEEE oraz CE</p>
13.	<p>Wraz z serwerami należy dostarczyć licencję na</p> <p>1. 4 x Windows Server 2022 Standard. Każda z licencji odpowiednia dla liczby rdzeni w zaoferowanym procesorze.</p> <p>2. Wraz z serwerami należy dostarczyć licencję na VMware Standard . Licencja odpowiednia dla liczby rdzeni w zaoferowanych serwerach na okres 2 lat.</p>

2. Przełącznik sieciowy typ 1 – 2 sztuki wraz z wdrożeniem.

Wdrożenie obejmuje:

- Montaż przełączników w szafie rack
- Konfigurację interfejsów zarządzających
- Konfigurację sieci VLAN
- Konfigurację sieci SAN (iSCSI)
- Podłączenie dostarczonej macierzy dyskowej oraz serwerów
- Podłączenie przełączników do infrastruktury Zamawiającego

LP.	Funkcjonalność
1.	Urządzenie musi być wyposażone w minimum 24 porty 10Gigabit Ethernet SFP+, 6 portów 40Gigabit Ethernet QSFP28 mogących pracować jako 100Gigabit Ethernet QSFP28 po instalacji dodatkowej licencji.
2.	Urządzenie musi być dostarczone z 1m DAC QSFP+ 40Gb, 4 x SFP+ 10Gb SR, 4 x SFP 1Gb RJ45;
3.	Urządzenie musi umożliwiać stworzenie wirtualnego systemu - złożonego z min. 2 przełączników szkieletowych będących przedmiotem opisu - zarządzanego jako jedno urządzenie logiczne. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów 10Gigabit Ethernet / 40 Gigabit Ethernet Ethernet oraz modułów optycznych lub kabli DAC. Musi istnieć możliwość terminowania połączeń link aggregation na dwóch przełącznikach tworzących taki system wirtualny (tzw. multi-chassis link aggregation)
4.	Urządzenie musi być wyposażone w wewnętrzne redundantne zasilacze 230V AC wspierające mechanizm HotSwap.
5.	Urządzenie musi być wyposażone w wewnętrzne redundantne wentylatory wspierające mechanizm HotSwap.
6.	Przepływ powietrza musi odbywać się od strony portów (zasysanie) w kierunku zasilaczy i modułów wentylacyjnych (wydmuch).
7.	<p>Wymagane parametry wydajnościowe:</p> <ul style="list-style-type: none"> a. Switching capacity: minimum 1 600 Gbps b. Forwarding capacity: minimum 480 Mpps c. min. 380 000 wpisów w tablicy adresów MAC d. min. 140 000 wpisów w tablicy ARP e. min. 190 000 wpisów w tablicy routingowej IPv4

	<ul style="list-style-type: none"> f. min. 80 000 wpisów w tablicy routingowej IPv6 g. min. 60 000 tras multicast h. min. 6 000 wpisów na potrzeby realizacji polityk bezpieczeństwa (listy kontroli dostępu ACL) i. min. 1 000 interfejsów VLAN j. min. 4 094 aktywnych sieci VLAN
8.	Obsługa protokołów warstwy 3 dla IPv4: Open Shortest Path First (OSPF), BGPv4, ISIS-IPv4
9.	Obsługa protokołów warstwy 3 dla IPv6: Open Shortest Path First (OSPFv3), BGP+, ISIS-IPv6
10.	Obsługuje protokoły multicastowe w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD
11.	Obsługuje protokoły MPLS, LDP, L2 i L3 VPN, VPLS, MPLS TE, MPLS.
12.	Musi umożliwiać rozbudowę o funkcjonalność VxLAN w przyszłości poprzez np.: zakup licencji
13.	<p>Urządzenie wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:</p> <ul style="list-style-type: none"> a. IEEE 802.1w Rapid Spanning Tree b. IEEE 802.1s Multiple Spanning Tree c. IEEE 802.3ad (Link Aggregation Control Protocol) umożliwiający grupowanie portów.
14.	<p>Urządzenie wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci (QoS):</p> <ul style="list-style-type: none"> a. Obsługa min. 8 kolejek per port, w tym co najmniej jedna kolejka ze statusem strict priority b. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP c. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP

	d. Definiowanie polityk QoS per port i per VLAN
15.	<p>Urządzenie wspiera następujące mechanizmy związane z bezpieczeństwem:</p> <ul style="list-style-type: none"> a. Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend b. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu c. Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard d. Weryfikacja źródła pakietu względem tablicy routingu (uRPF) – zarówno dla IPv4 i IPv6 e. Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP f. Listy kontroli dostępu także dla IPv6 g. Mechanizmy ochrony warstwy kontrolnej
16.	Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame)
17.	Urządzenie przystosowane do montażu w szafie 19", wysokość nie większa niż 1RU, elementy niezbędne do montażu muszą być dostarczone z urządzeniem
18.	<p>Urządzenie musi wspierać następujące mechanizmy związane z zarządzaniem:</p> <ul style="list-style-type: none"> a. Ma możliwość zarządzania przez WEB Gui (HTTPS), SNMPv3 oraz SSHv2 b. Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Ethernet out-of-band management c. Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+ d. Posiada port USB e. Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie (SPAN,RSPAN), polegającą na kopiowaniu pojawiających się na

	<p>nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN</p> <p>f. Posiada możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow, sFlow lub odpowiednik).</p> <p>g. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych</p>
19.	Urządzenie musi być wyposażone w zintegrowany kontroler sieci WLAN zdolny do pracy w klastrze HA przy utworzeniu stosu przełączników.
20.	Wbudowany serwer DHCP obsługujący co najmniej 64 pule adresów IP
21.	Obsługa funkcji DHCP klient i DHCP relay
22.	Obsługa funkcji: ochrony serwera DHCP, DHCP snooping, Dynamic ARP Inspection, IP Source Guard
23.	Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
24.	Obsługa 802.3ad Link Aggregation Protocol (LACP)
25.	Funkcja BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPUs w celu przeciwdziałania pętlom
26.	Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
27.	Obsługa routingu statycznego i dynamicznego (co najmniej protokoły: RIP, OSPF, ISIS, BGP)
28.	Obsługa routingu bazującego na politykach (Policy Based Routing)
29.	Obsługa IGMP v1/v2/v3 oraz IGMP snooping i IGMP proxy
30.	Obsługa protokołu PIM-SM
31.	Funkcja izolacji użytkowników radiowych (wewnątrz grupy a także

	między grupami użytkowników)
32.	Funkcja automatycznego zwiększania mocy pobliskich AP w przypadku awarii jednego z nich w celu zapewnienia pełnego pokrycia sygnałem WiFi
33.	Obsługa sieci IEEE 802.1Q VLAN – minimum 4 000 sieci VLAN obsługiwanych równocześnie
34.	Zarządzanie poprzez wbudowane Web GUI jak i możliwe zarządzanie przy pomocy zewnętrznego serwera z Web GUI
35.	Zarządzanie poprzez port konsoli (CLI)
36.	Wsparcie dla SNMP v1/v2/v3
37.	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
38.	Wymagany jest serwis gwarancyjny świadczony przez minimum 3 lata. Dostępność serwisu 9x5xNBD. W trakcie trwania serwisu zapewniony dostęp do poprawek i nowych wersji oprogramowania
39.	Gwarantowany czas naprawy sprzętu – 48h od momentu zgłoszenia i potwierdzenia awarii.

3. Przełącznik sieciowy typ 2 – 2 sztuki wraz z wdrożeniem.

Wdrożenie obejmuje:

- Montaż przełączników w szafie rack
- Konfigurację interfejsów zarządzających
- Konfigurację sieci VLAN
- Podłączenie przełączników do infrastruktury Zamawiającego
- Podłączenie urządzeń końcowych do dostarczonych przełączników

LP.	Funkcjonalność
1.	Urządzenie musi być wyposażone w minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T ze wsparciem dla trybów: full-duplex, half-duplex, automatycznej negocjacji (auto-negotiation).
2.	Urządzenie musi być wyposażone w minimum 4 porty 1/10Gb SFP/SFP+, pozwalające na instalację wkładek 10Gb (SFP+), Gigabitowych (SFP) oraz kabli DAC/Twinax SFP+.
3.	Urządzenie musi być dostarczone z modułami SFP+ w następującej konfiguracji: 4 sztuki 10G SR, 1 przewód DAC SFP+ o długości 1m
4.	Urządzenie musi umożliwiać stworzenie wirtualnego systemu - złożonego z

	<p>min. 8 przełączników zarządzanego jako jedno urządzenie logiczne.</p> <p>Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów 10Gigabit Ethernet oraz modułów optycznych lub kabli DAC. Musi istnieć możliwość terminowania połączeń link aggregation na dwóch przełącznikach tworzących taki system wirtualny (tzw. multi-chassis link aggregation)</p>
5.	Urządzenie musi być wyposażone w wewnętrzne redundantne zasilacze 230V AC wspierające mechanizm HotSwap.
6.	<p>Wymagane parametry wydajnościowe:</p> <ul style="list-style-type: none"> a. Switching capacity: minimum 176 Gbps b. Forwarding capacity: minimum 125 Mpps c. min. 64 000 wpisów w tablicy adresów MAC d. min. 16 000 wpisów w tablicy ARP e. min. 32 000 wpisów w tablicy routingu IPv4 f. min. 8 000 wpisów w tablicy routingu IPv6 g. min. 2 000 wpisów na potrzeby realizacji polityk bezpieczeństwa (listy kontroli dostępu ACL) h. min. 1 000 interfejsów VLAN i. min. 4 094 aktywnych/jednoczesnych sieci VLAN
7.	Obsługa protokołów warstwy 3 dla IPv4: Open Shortest Path First (OSPF), BGPv4, ISIS-IPv4
8.	Obsługa protokołów warstwy 3 dla IPv6: Open Shortest Path First (OSPFv3), BGP4+, ISIS-IPv6
9.	Obsługuje protokoły multicastowe w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD
10.	<p>Urządzenie wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:</p> <ul style="list-style-type: none"> a. IEEE 802.1w Rapid Spanning Tree b. IEEE 802.1s Multiple Spanning Tree c. IEEE 802.3ad (Link Aggregation Control Protocol) umożliwiający grupowanie portów.
11.	Urządzenie wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci (QoS):

	<ul style="list-style-type: none"> a. Obsługa min. 8 kolejek per port, w tym co najmniej jedna kolejka ze statusem strict priority b. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP c. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP d. Definiowanie polityk QoS per port i per VLAN
12.	<p>Urządzenie wspiera następujące mechanizmy związane z bezpieczeństwem:</p> <ul style="list-style-type: none"> a. Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend b. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu c. Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard d. Weryfikacja źródła pakietu względem tablicy routingu (uRPF) – zarówno dla IPv4 i IPv6 e. Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP f. Listy kontroli dostępu także dla IPv6 g. Mechanizmy ochrony warstwy kontrolnej
13.	Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame)
14.	Przystosowane do montażu w szafie 19", wysokość nie większa niż 1RU, elementy niezbędne do montażu muszą być dostarczone z urządzeniem
15.	Urządzenie musi wspierać następujące mechanizmy związane z zarządzaniem:

	<ul style="list-style-type: none"> a. Ma możliwość zarządzania przez WEB Gui (HTTPS), SNMPv3 oraz SSHv2 b. Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Ethernet out-of-band management c. Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+ d. Posiada port USB e. Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie (SPAN,RSPAN), polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN f. Posiada możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow, sFlow lub odpowiednik) g. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych
16.	<p>Wymagany jest serwis gwarancyjny świadczony przez minimum 3 lata. Dostępność serwisu 9x5xNBD. W trakcie trwania serwisu zapewniony dostęp do poprawek i nowych wersji oprogramowania</p>

4. System zarządzający kopią bezpieczeństwa wraz z wdrożeniem.

Wdrożenie obejmujące:

- a. Instalacja systemu na udostępnionym przez Zamawiającego serwerze fizycznym.
- b. Instalację niezbędnych komponentów wymaganych do poprawnej konfiguracji zadań kopii bezpieczeństwa.
- c. Konfiguracja zadań kopii bezpieczeństwa zgodnie z najlepszymi praktykami.
- d. Konfiguracja dostarczonej przez Zamawiającego biblioteki taśmowej.
- e. Konfiguracja kopii bezpieczeństwa na dostarczoną przez Zamawiającego bibliotekę taśmową.

- f. Konfiguracja automatycznego, cyklicznego zadania testowego odtwarzania wskazanych przez Zamawiającego systemów wraz z generowaniem raportów z wykonania zadania.

LP.	Funkcjonalność
1.	<p>Wymagania ogólne</p> <ul style="list-style-type: none">a. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Dostarczona licencja musi być licencją wieczystą ze wsparciem minimum 1 rok. Dostarczona licencja musi pozwalać na ochronę minimum 40 maszyn wirtualnych.b. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x i 8.x oraz Microsoft Hyper-V 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczejc. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
2.	<p>Całkowite koszty posiadania</p> <ul style="list-style-type: none">a. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowejb. Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych blokówc. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacjid. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być

przechowywane w plikach backupu.

- e. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych w takiej puli.
- f. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
- g. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
- h. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- i. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
- j. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
- k. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
- l. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- m. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji

	<ul style="list-style-type: none"> n. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania o. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. p. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej q. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora) r. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS) s. Oprogramowanie musi posiadać integracje z systemami typu SIEM t. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. <p>Powinna istnieć możliwość wyłączenia tej opcji.</p>
3.	<p>Wymagania RPO</p> <ul style="list-style-type: none"> a. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej b. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. c. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastora d. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia

	<p>jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.</p> <ul style="list-style-type: none"> e. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. f. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). g. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) h. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, Quantum DXi i. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. j. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. k. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. l. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO. m. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik n. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji
--	---

	<p>(replica seeding)</p> <p>o. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)</p>
4.	<p>Wymagania RTO</p> <p>a. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.</p> <p>b. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)</p> <p>c. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami</p> <p>d. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere</p> <p>e. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.</p> <p>f. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków</p> <p>g. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack,</p>

Amazon EC2 oraz Google Cloud Platform.

- h. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynie operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- i. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- j. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
- k. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
- l. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- m. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
- n. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
- o. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
- p. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych

	<p>witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.</p> <p>q. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.</p> <p>r. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.</p> <p>s. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji</p> <p>t. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN</p> <p>u. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle</p> <p>v. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI</p> <p>w. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2</p> <p>x. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN</p>
5.	<p>Ograniczenie ryzyka</p> <p>a. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)</p> <p>b. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.</p>

	<ul style="list-style-type: none"> c. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem d. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. e. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware f. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania g. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków h. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
6.	<p>Środowiska fizyczne</p> <ul style="list-style-type: none"> a. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego b. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych c. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE d. Rozwiązanie musi wspierać system operacyjny macOS

	<ul style="list-style-type: none"> e. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix f. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również scentralizowany (poprzez centralną konsolę zarządzającą) g. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster h. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów i. Rozwiązanie musi wspierać backup podłączonych dysków USB j. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym k. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) l. Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone m. Rozwiązanie musi wspierać kontrolę pasma sieciowego n. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych o. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN p. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft q. Rozwiązanie musi wspierać technologię BitLocker
--	---

	<ul style="list-style-type: none"> r. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania s. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2016 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych t. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych u. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. v. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform w. Rozwiązanie musi wspierać szyfrowanie x. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne y. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego z. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej aa. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
--	--

5. Klaster firewall- System UTM – 2 sztuki wraz z wdrożeniem.

Wdrożenie obejmuje:

- a. Instalację dostarczonych systemów w infrastrukturze Zamawiającego.
- b. Konfigurację klastra HA active-active
- c. Odtworzenie konfiguracji z posiadanych przez Zamawiającego systemów FG300D oraz Stormshield na zainstalowanym systemie

- d. Konfigurację polityk bezpieczeństwa
- e. Konfigurację połączeń VPN
- f. Konfigurację routingu
- g. Po przeprowadzanej instalacji i konfiguracji wymagane jest przeszkolenie administratora z całości systemu UTM ze szczególnym uwzględnieniem nowych funkcjonalności.

LP.	Funkcjonalność
1.	<p>Wymagania Ogólne</p> <ul style="list-style-type: none"> a. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. b. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. c. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. d. System wspiera protokoły IPv4 oraz IPv6 w zakresie: <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
2.	<p>Redundancja, monitoring i wykrywanie awarii</p> <ul style="list-style-type: none"> a. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia

	<p>funkcję synchronizacji sesji.</p> <p>b. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</p> <p>c. Monitoring stanu realizowanych połączeń VPN.</p> <p>d. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</p>
3.	<p>Interfejsy, Dysk, Zasilanie:</p> <p>a. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:</p> <ul style="list-style-type: none"> • 16 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 2 gniazdami SFP+ 10 Gbps. <p>b. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</p> <p>c. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>d. System jest wyposażony w zasilanie AC.</p>
4.	<p>Parametry wydajnościowe:</p> <p>a. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.</p> <p>b. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.</p> <p>c. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B.</p> <p>d. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.</p> <p>e. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.</p> <p>f. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.</p>

	<ul style="list-style-type: none"> g. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps. h. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. i. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
5.	<p>Funkcje Systemu Bezpieczeństwa:</p> <p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> a. Kontrola dostępu - zaporę ogniową klasy Stateful Inspection. b. Kontrola Aplikacji. c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. d. Ochrona przed malware. e. Ochrona przed atakami - Intrusion Prevention System. f. Kontrola stron WWW. g. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. h. Zarządzanie pasmem (QoS, Traffic shaping). i. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). j. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. k. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. l. Analiza ruchu szyfrowanego protokołem SSH. m. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

	<p>n. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).</p>
6.	<p>Polityki, Firewall</p> <p>a. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>b. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <ul style="list-style-type: none"> • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. <p>c. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>d. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</p> <p>e. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>f. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p>
7.	<p>Połączenia VPN</p> <p>a. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługę protokołu Diffie-Hellman grup 19, 20 oraz 21. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Dynamiczne zestawianie tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich

	<p>aktywności.</p> <ul style="list-style-type: none"> • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>b. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
8.	<p>Funkcje SD-WAN</p> <ol style="list-style-type: none"> a. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. b. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). c. Reguły SD-WAN umożliwiają określenie aplikacji jako argumentu dla kierowania ruchu. d. Rozwiązanie powinno wspierać funkcję Forward Error Correctionm na

	<p>tunelach IPSec.</p> <p>e. Funkcja monitorowania łączy w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.</p>
9.	<p>Zarządzanie pasmem</p> <p>a. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>b. System daje możliwość określania pasma dla poszczególnych aplikacji.</p> <p>c. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>d. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
10.	<p>Ochrona przed malware</p> <p>a. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>b. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, SMTP, CIFS.</p> <p>c. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.</p> <p>d. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>e. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>f. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>g. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami</p>

	<p>lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.</p> <p>h. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>i. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>j. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>
11.	<p>Ochrona przed atakami</p> <p>a. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>b. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>c. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>d. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>e. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>f. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>g. Możliwość kontrolowania długości nagłówka, liczby parametrów URL oraz Cookies dla protokołu http.</p> <p>h. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>i. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>
12.	<p>Kontrola aplikacji</p> <p>a. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów</p>

	<p>TCP/UDP.</p> <ul style="list-style-type: none"> b. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. c. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. d. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. e. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. f. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). g. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
13.	<p>Kontrola WWW</p> <ul style="list-style-type: none"> a. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. b. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. c. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. d. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. e. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). f. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

	<p>g. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>h. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.</p> <p>i. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>j. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p> <p>k. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów: youtube, vimeo.</p> <p>l. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.</p>
14.	<p>Uwierzytelnianie użytkowników w ramach sesji</p> <p>a. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <p>b. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>c. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</p> <p>d. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
15.	<p>Zarządzanie</p> <p>a. Elementy systemu bezpieczeństwa muszą mieć możliwość</p>

	<p>zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <ul style="list-style-type: none"> b. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. c. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. d. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. e. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. f. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. g. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. h. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). i. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
16.	<p>Logowanie</p> <ul style="list-style-type: none"> a. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. b. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość

	<p>jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>c. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>d. Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>e. System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>f. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
17.	<p>Serwisy i licencje</p> <p>Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:</p> <p>a. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.</p>
18.	<p>Gwarancja oraz wsparcie</p> <p>a. System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</p>
19.	<p>Rozszerzone wsparcie serwisowe AHB/SOS</p> <p>a. System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.</p> <p>System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <ul style="list-style-type: none"> • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.

	<ul style="list-style-type: none"> • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). • Przygotowanie urządzenia do zdalnej konfiguracji. • Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. • wsparcie techniczne wymaganego serwisu. • Należy posiadać Certyfikat ISO 9001 podmiotu serwisującego.
20.	Voucher na szkolenie dla administratora autoryzowane przez producenta rozwiązania, certyfikat wydany przez producenta potwierdzający odbycie szkolenia, czas trwania min:4 dni, voucher do wykorzystania przez 12 m-cy

6. Zasilacz awaryjny UPS – 1 szt

W skład zasilacza wchodzi:

Zasilacz awaryjny UPS przystosowany do montażu w szafach typu rack 19" wraz z uchwyty montażowymi do szaf rack 19" oraz zestawem przewodów zasilających oraz sygnałowych.

Do protokołu odbioru należy załączyć karty katalogowe lub działające linki do strony internetowej

producenta, które prowadzą do kart katalogowych zasilacza awaryjnego UPS.

LP.	Funkcjonalność	
-----	----------------	--

1.	Moc wyjściowa: 8000W / 8000VA.	
2.	Napięcie wyjściowe: 230V.	
3.	Maksymalna możliwa do konfiguracji moc: 8000W / 8000VA.	
4.	Zniekształcenie harmoniczne: mniej niż 3%.	
5.	Częstotliwość na wyjściu (synchronicznie z siecią): 57–63Hz przy częstotliwości nominalnej 60Hz.	
6.	Topologia: Podwójna konwersja (online).	
7.	Typ przebiegu: sinusoida.	
8.	Gniazda wyjściowe: a. IEC 320 C13 - 6 sztuk, b. IEC 320 C19 - 4 sztuki, c. IEC Jumpers - 3 sztuki.	
9.	Nominalne napięcie wejściowe: 230V / 400V	
10.	Częstotliwość na wejściu: 40/70Hz (automatyczne wykrywanie).	
11.	Typ gniazda wejściowego: połączenie poprzez zacisk 3-przewodowy.	
12.	Inne napięcia wejściowe: 220V, 240V.	
13.	Limit napięcia wejściowego: 140V - 275V.	
14.	Typ akumulatora: bezobsługowy akumulator kwasowo-ołowiowy.	
15.	Typowy czas pełnego ładowania akumulatora: 2 godziny.	
16.	Oczekiwana żywotność akumulatora: 3 - 5 lat.	
17.	Czas podtrzymania dla obciążenia 100%: minimum 5 minut.	
18.	Czas podtrzymania dla obciążenia 50%: minimum 14 minut.	
19.	Możliwość podłączenia zewnętrznych modułów bateryjnych.	
20.	Port komunikacyjny: UPS wyposażony w kartę do zdalnego zarządzania z gniazdem RJ45.	

21.	Panel przedni: wielofunkcyjna konsola sterownicza i informacyjna LCD.	
22.	Obudowa: przystosowana do mocowania w szafie RACK 19", dostarczona wraz z szynami umożliwiającymi montaż urządzenia w szafie RACK 19".	
23.	Maksymalna wysokość: 6U.	
24.	Temperatura pracy: 0 °C - 40 °C.	
25.	Wilgotność względna podczas pracy: 0% - 95%.	
26.	Temperatura (przechowywanie): -15 °C - +45 °C,	
27.	Potwierdzenia zgodności: CE, VDE, IRAM, EN/IEC 62040-1:2019/A11:2021, EN/IEC 62040-2:2006/AC:2006, EN/IEC 62040-2:2018.	
28.	Okres gwarancji: minimum 2 lata gwarancji na zasilacz oraz 2 lata na moduły bateryjne.	

W ramach niniejszego postępowania Zamawiający wymaga podłączenia, skonfigurowania i uruchomienia zaoferowanego urządzenia UPS do sieci elektrycznej Urzędu celem zabezpieczenia pomieszczenia serwerowni. Wszystkie koszty z tym związane np.: modernizacji istniejącej instalacji elektrycznej muszą zostać przewidziane i uwzględnione w ofercie Wykonawcy.

7. Zasilacz awaryjny UPS – 6 szt

Do protokołu odbioru należy załączyć karty katalogowe lub działające linki do strony internetowej producenta, które prowadzą do kart katalogowych zasilacza awaryjnego UPS.

LP.	Nazwa komponentu	Wymagania minimalne
1.	Moc pozorna	1400 0VA
2.	Moc rzeczywista	700 VA

3.	Napięcie znamionowe	230 V
4.	Częstotliwość znamionowa	50 Hz
5.	Kształt napięcia	Sinusoidalny
6.	Napięcie znamionowe wyjściowe	230 V
7.	Częstotliwość wyjściowa	50 Hz
8.	Typ obudowy	Wolnostojący
9.	Wyposażenie	UPS, instrukcja obsługi (może być w postaci elektronicznej), instrukcja bezpieczeństwa. - 1 x kabel komunikacyjny USB 1 x kabel zasilający - wejściowy

Wymagania pozostałe:

1. Dostarczone sprzęty i oprogramowanie muszą być kompletne i muszą posiadać wszelkie wymagane instrukcje, gwarancje i licencje.

2. Oferta musi być jednoznaczna i kompleksowa, tj.: obejmować cały asortyment proponowanego przedmiotu zamówienia. Przedmiot zamówienia musi być kompletny, ze wszystkimi podzespołami, częściami i materiałami niezbędnymi do uruchomienia i użytkowania sprzętu zgodnie z jego przeznaczeniem. Oferowany przedmiot zamówienia musi spełniać wymogi Zamawiającego.

3. Wykonawca może zaoferować sprzęt o parametrach nie gorszych lub lepszych niż opisane, jednak w żadnym stopniu nie obniżający standardu i nie zmieniający rozwiązań technicznych podanych w OPZ, a tym samym nie pozbawiający Zamawiającego żądanych wydajności, funkcjonalności, użyteczności opisanego sprzętu. Wskazanie przez Zamawiającego w SWZ marek lub nazw handlowych towarów ma charakter wyłącznie przykładowy, pomocniczy dla określenia klasy produktu, a nie wskazuje na konkretny wyrób lub konkretnego producenta. Wykonawca przy sporządzeniu oferty kieruje się wyłącznie wymaganiami co do parametrów towarów, a nie ma obowiązku oferowania towarów podanych jako przykładowe. W przypadku zaoferowania oprogramowania równoważnego,

na wykonawcy spoczywa obowiązek udowodnienia, że uprawnienia Zamawiającego wynikające z posiadanych przez niego licencji oraz cechy oferowanego oprogramowania są równoważne w stosunku do oprogramowania określonego w OPZ. W tym celu wykonawca zobowiązany jest załączyć opis i dane techniczne zaproponowanego rozwiązania, umożliwiające porównanie go z wszystkimi parametrami, wymaganymi opisem przedmiotu zamówienia, w tym zgodność posiadanego przez Zamawiającego oprogramowania z zaproponowanym rozwiązaniem.

W przypadku, gdy zaoferowane przez wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego 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 odinstalowaniu oprogramowania równoważnego.

4. Oprogramowanie musi być zaoferowane w najnowszych, obecnie dostępnych wersjach.

5. Dostawa przedmiotu zamówienia odbywać się będzie na koszt i ryzyko wykonawcy na miejsce wskazane przez Zamawiającego. Urządzenia dostarczane będą bez plombowanych obudów z oznakowanymi podzespołami głównymi z możliwością instalacji rozszerzeń bez utraty gwarancji. Z chwilą dostarczenia przedmiotu zamówienia przejdą na Zamawiającego korzyści i ciężary związane z przedmiotem zamówienia oraz niebezpieczeństwo jego przypadkowej utraty lub uszkodzenia. Sprzęt ma być dostarczony w oryginalnych opakowaniach producenta

6. Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.

7. Dla oprogramowania musi być publicznie znany cykl życia przedstawiony przez producenta systemu i dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie przez producenta na jego stronie internetowej w okresie co najmniej 5 lat.

8. Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta.

9. Urządzenia będące przedmiotem zamówienia muszą być fabrycznie nowe, nieużywane, w pełni sprawne i wolne od wad fizycznych. Przedmiot umowy nie może być obciążony prawami osób trzecich.

10. Cały sprzęt musi mieć kompletne odpowiednie okablowanie niezbędne do uruchomienia poszczególnych urządzeń.

11. Wszystkie elementy określone w opisie przedmiotu zamówienia muszą stanowić integralną część urządzeń. Zamawiający nie dopuszcza możliwości konfigurowania sprzętu za pomocą elementów zewnętrznych, za wyjątkiem sytuacji, gdy opis przedmiotu zamówienia wyraźnie na to wskazuje

12. Wszystkie urządzenia objęte zamówieniem muszą być fabrycznie nowe, w możliwie najwyższej klasie jakości, nieużywane, nieregenerowane, kompletne, wyprodukowane nie wcześniej niż w styczniu 2023 r. oraz dostarczone w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”.

13. Oprogramowanie objęte zamówieniem musi być nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej najwyższej stabilnej wersji i pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych. Zamawiający zastrzega możliwość przeprowadzenia weryfikacji oryginalności dostarczonego oprogramowania u Producenta w przypadku wystąpienia wątpliwości co do jego legalności.