KRAJOWY PLAN ODBUDOWY

ZAPYTANIE OFERTOWE

w postępowaniu prowadzonym
zgodnie z zasadą konkurencyjności

Zamówienie w ramach projektu pn *„Wdrożenie do firmy Paged Morąg SA. kompletnego cyberfizycznego systemu, umożliwiającego cyfryzację i robotyzację produkcji sklejki i wprowadzenie założeń przemysłu 4.0. na rzecz zwiększenia odporności do działania w warunkach kryzysowych”* współfinansowane z **KRAJOWEGO PLANU ODBUDOWY, A2.1.1 - Inwestycje wspierające robotyzację i cyfryzację w przedsiębiorstwach**

PRZEDMIOT ZAMÓWIENIA:

Kompleksowy system do tworzenia kopii zapasowych oraz ochrony przed atakami szyfrującymi dane

ZAMAWIAJĄCY:

Paged Morąg S. A.
14-300 Morąg, ul. Mazurska 1,
NIP 7411378488, REGON 510445569

System będzie obejmował Zakład Produkcji Sklejki w Piszu i Zakład Produkcji Sklejki Morągu

1. **OPIS PRZEDMIOTU ZAMÓWIENIA**

kod CPV: 32420000-3 - Urządzenia sieciowe, 48820000-2 - Serwery

Załącznik nr 4 (poniżej) „Specyfikacja Istotnych Warunków Zamówienia” opisuje szczegółowe wymagania dotyczące zamawianego systemu. W szczególności zapytanie obejmuje:

- **sprzęt do filtrowania i ochrony sieci**
  umożliwiający ochronę i separację pozostałych urządzeń;
- **serwer piaskownicy**
  pozwalający weryfikować skuteczność kopii oraz testowo odtwarzać środowisko;
- **serwer do analizy danych**
  służący do bieżącej analizy tworzonych kopii zapasowych, w tym do wykrywania ataków i anomalii w danych;
- **biblioteka dyskowa**
  stanowiąca składnicę i archiwum danych;
- **dwa deduplikatory wraz z oprogramowaniem do tworzenia kopii zapasowych oraz niezbędne licencje**
  zestawy pozwalające na efektywne wykonywanie kopii zapasowych w oparciu o rzeczywiste zmiany danych, uwzględniając powtarzalność części danych oraz ograniczając obciążenie sieci do niezbędnego minimum;
- **wdrożenie, przeszkolenie i wsparcie powdrożeniowe**.

W przypadku, gdzie Zamawiający posługuje się w opisie przedmiotu zamówienia, we wszystkich dokumentach i załącznikach opisujących przedmiot zamówienia nazwami konkretnych producentów, nazwami konkretnych produktów, znakami towarowymi, patentami czy pochodzeniem, należy to traktować jedynie jako pomoc w opisie przedmiotu zamówienia – mają one jedynie przybliżyć wymagania, których nie można było opisać przy użyciu dostatecznie dokładnych i zrozumiałych określeń. W każdym przypadku dopuszcza się użycie produktu równoważnego, który spełni minimalne standardy jakościowe, parametry techniczne, warunki docelowego przeznaczenia oraz funkcji i walorów użytkowych produktu wskazanego z nazwy.

W każdym przypadku dopuszcza się możliwość zastosowania materiałów, komponentów równoważnych wobec wskazanych w opisie przedmiotu zamówienia oraz załącznikach pod warunkiem zachowania ich zgodności z planowanym przeznaczeniem i obowiązującymi przepisami, które spełniają minimalne standardy jakościowe, parametry techniczne, warunki docelowego przeznaczenia oraz funkcje i walory użytkowe.

W związku z przyjętym harmonogramem realizacji inwestycji, w przypadku pytań lub wątpliwości co do przedmiotu zamówienia, prosimy o kierowanie zapytań najpóźniej do pięciu dni przed terminem składania ofert.

2. WARUNKI UDZIAŁU W POSTĘPOWANIU

Oferty mogą składać Wykonawcy, którzy:

1. dysponują potencjałem technicznym, koniecznym do należytego wykonania zamówienia;
2. realizacji umowy maksymalnie 18 tyg. od dnia podpisania umowy.
3. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia;
4. posiadają wykwalifikowaną kadrę, gotową do realizacji zamówienia;
5. posiadają niezbędną wiedzę i doświadczenie oraz zdolności techniczne i organizacyjne umożliwiające prawidłowe wykonanie przedmiotu zamówienia;
6. nie posiadają powiązania osobowe lub kapitałowe z Zamawiającym – przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Beneficjenta lub osobami wykonującymi w imieniu Beneficjenta czynności związanych z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:
   - uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
   - posiadanie co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa);
   - pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
   - pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawanie we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia;
   - pozostawanie z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

3. KRYTERIA OCENY OFERTY I WAGI PROCENTOWE

Oferty będą oceniane wg następujących kryteriów:

1. 75% – cena;
2. 25% – termin dostawy i realizacji.

Z postępowania zostaną wykluczone oferty, które:

1. nie spełniają warunków umieszczonych w zapytaniu ofertowym, w tym w specyfikacji istotnych warunków zamówienia;
2. pochodzą od wykonawców mających powiązania osobowe lub kapitałowe z Zamawiającym;
3. zawierają istotne błędy w obliczeniu ceny lub cena oferty jest rażąco niska – w takiej sytuacji Zamawiający może poprosić o uzupełnienie oferty o dokumenty potwierdzające możliwość realizacji oferty w tej cenie;
4. zostaną złożone po wskazanym terminie;

5. będą zawierały zbyt długi termin realizacji uniemożliwiający finansowanie w ramach projektu KPO.

4. OPIS SPOSOBU PRZYZNAWANIA PUNKTACJI ZA SPEŁNIENIE DANEGO KRYTERIUM OCENY OFERTY.

3.1. kryterium ceny uwzględniające wszystkie niewykluczone oferty, zgodnie ze wzorem:
$C_{\%} = \frac{3(C_n - C_{min})}{4(C_{max} - C_{min})}$, w szczególności: najniższa cena 75%, najwyższa cena 0%;

3.2. termin dostawy i realizacji liczony od dnia podpisania umowy:
   a. 25% – do 7 tygodni;
   b. 15% – 7-10 tygodni;
   c. 5% – 10-14 tygodni;
   d. 0% – powyżej 14 tygodni.

5. MIEJSCE ORAZ TERMIN SKŁADANIA OFERT

Oferty prosimy składać do 10 lutego 2025 r na adresy:

tomasz.oldakowski@paged.pl krzysztof.mykowski@paged.pl

6. INFORMACJA O MOŻLIWOŚCI SKŁADANIA OFERT CZĘŚCIOWYCH

Zamawiający nie dopuszcza możliwości składania ofert częściowych.

7. INFORMACJĘ O PLANOWANYCH ZAMÓWIENIACH UZUPEŁNIAJĄCYCH

Zadamawiający nie planuje zamówień uzupełniających.

8. TERMIN REALIZACJI UMOWY

Maksymalnie 18 tyg. od dnia podpisania umowy.

9. ISTOTNE POSTANOWIENIA UMOWY I WARUNKI ZMIANY ISTOTNYCH POSTANOWIEŃ UMOWY

Zamawiający wymaga, aby Wykonawca, którego oferta zostanie uznana za najkorzystniejszą, zawarł umowę zgodnie z treścią zapytania. Wykonawca ma prawo zaproponować wzór umowy stosowany w praktyce handlowej. Zamawiający dopuszcza wypłatę zaliczki na poczet realizacji zamówienia w kwocie uzgodnionej z Wykonawcą nie wyższą niż 50% ceny ujawnionej przez Wykonawcę w ofercie.

Podstawą rozliczeń między stronami będą faktury.

10. WARUNKI EWENTUALNEGO ODSTĄPIENIA OD ZAWARCIA UMOWY

W przypadku gdy zaoferowana cena przekracza kwotę środków przeznaczonych przez Zamawiającego na realizację zamówienia Zamawiający może unieważnić postępowanie i odstąpić od podpisania umowy.

11. ZAŁĄCZNIKI

Oferty prosimy składać wraz z wypełnionymi załącznikami:

Załącznik 1 – Formularz oferty

W odpowiedzi na Zapytanie Ofertowe dot. *Kompleksowego systemu do tworzenia kopii zapasowych oraz ochrony przed atakami szyfrującymi dane sklejki* składamy poniższą ofertę:

Dane oferenta	
Nazwa	
Adres	
NIP	
Nr KRS lub CEIDG	
Nr rejestrowy dla kraju innego niż PL	
Dane osoby kontaktowej	
Imię i nazwisko	
Adres e-mail	
Telefon	
Określenie do kryteriów wyboru ofert	
Wartość oferty netto w PLN	
Termin realizacji liczony w miesiącach od daty podpisania umowy	

Załącznik 2 – Oświadczenie o spełnieniu wszystkich warunków udziału w postępowaniu

1. Dysponuję potencjałem technicznym, koniecznym do należytego wykonania zamówienia.
2. Znajduję się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
3. Posiadam wykwalifikowaną kadrę, gotową do realizacji zamówienia.
4. Posiadam niezbędną wiedzę i doświadczenie oraz zdolności techniczne i organizacyjne umożliwiające prawidłowe wykonanie przedmiotu zamówienia.

Załącznik 3 – Oświadczenie o braku powiązań osobowych i kapitałowych

Oświadczam(y), że nie jestem(eśmy) powiązani z Zamawiającym osobowo lub kapitałowo.

.....

data i podpis przedstawiciela Wykonawcy (dotyczy wszystkich 3 załączników)

Załącznik 4 – Specyfikacja istotnych warunków zamówienia (SIWZ)

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Wszystkie poniższe wymagania opisują minimalne parametry, które musi spełniać oferta.

1. Wymagania ogólne
   - 1.1. system ma działać bezprzerwowo 24/h na dobę 7 dni w tygodniu;
   - 1.2. kopie zapasowe powinny być zapisywane lokalnie oraz co najmniej w 1 dodatkowej lokalizacji;
   - 1.3. w przypadku awarii pojedynczego urządzenia reszta infrastruktury powinna nadal działać, a odzyskanie / przywrócenie kopii powinno być możliwe z urządzenia w innej lokalizacji;
   - 1.4. aktualizacje oprogramowania („software"), w tym oprogramowania układowego („firmware") powinno odbywać się automatycznie w taki sposób, aby urządzenia w każdej lokalizacji były aktualizowane w innych przedziałach czasu;
   - 1.5. w razie potrzeby wsparcie techniczne powinno być udzielane najpóźniej w następnym dniu roboczym po zgłoszeniu zapotrzebowania;
   - 1.6. w ramach gwarancji naprawa lub wymiana urządzeń powinna odbywać się w ciągu 14 dni roboczych.
2. Sprzęt do filtrowania ruchu i ochrony sieci „ROUTER-FIREWALL"
   - 2.1. Router musi obsługiwać:
     - 2.1.1. programowe wyłączanie interfejsów komunikacyjnych (portów);
     - 2.1.2. filtrowanie ruchu IPv4 i IPv6 („firewall");
     - 2.1.3. szyfrowanie i tunelowanie połączeń przez IPSec VPN („virtual private network");
     - 2.1.4. wykrywanie wirusów za pomocą sygnatur i heurystyki;
     - 2.1.5. wykrywanie intruzów („intrusion prevention system" – „IPS");
     - 2.1.6. kontrolę na poziomie warstwy aplikacji („layer 7 firewall");
   - 2.2. Router musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji w każdej z wymienionych technologii, a każda instancja powinna mieć możliwość zarządzania przez co najmniej 5 administratorów o dedykowanych poświadczeniach;
   - 2.3. Router musi obsługiwać redundancję i powinien być skonfigurowany w klaster w taki sposób, aby w przypadku awarii 1 urządzenia jego rolę przejęło 2 urządzenie (klaster „active-active" lub „active-pasive") – klaster musi zapewniać synchronizację sesji (w ramach „firewall" i połączeń „VPN");
   - 2.4. Router musi posiadać:
     - 2.4.1. 10 fizycznych portów o prędkości 10Gbps;
     - 2.4.2. port USB umożliwiające instalację (aktualizację) oprogramowania;
     - 2.4.3. możliwość konfiguracji po minimum 200 interfejsów wirtualnych, w tym VLAN'y zgodne ze standardem 802.1Q;
     - 2.4.4. możliwość równoczesnego zasilania z 2 niezależnych źródeł 230V AC zapewniającą ciągłość pracy w przypadku odłączenia 1 ze źródeł zasilania.
   - 2.5. Minimalna wydajność routera:
     - 2.5.1. przełączanie („switching") równocześnie 170 milionów pakietów (wielkości 64-bitów), szybkość przełączania 240Gbps („fast-forward");
     - 2.5.2. obsługa 700 tys. jednoczesnych połączeń („connection tracking");
     - 2.5.3. obsługa 32 tys. nowych połączeń na sekundę;

2.5.4. przepustowość 10Gbps dla pakietów 512B w ramach „Stateful firewall";
2.5.5. przepustowość 1.7Gbps przy włączonym filtrowaniu w warstwie aplikacji;
2.5.6. wydajność IPsec 6Gbps przy użyciu protokołu AES z kluczem 128-bitów;
2.5.7. wydajność dwukierunkowego skanowania ruchu 1.3Gbps w ramach wykrywania włamań („IPS");
2.5.8. wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw 650Mbps przy jednocześnie włączonych IPS, kontroli aplikacji i ochronie antywirusowej (ruch typu „Enterprise Traffic Mix", „Enterprise Testing Condition")
2.5.9. obsługa standardów:
- IEEE 802.3 10BASE-T Ethernet;
- IEEE 802.3u 100BASE-TX Fast Ethernet;
- IEEE 802.3ab;
- 1000BASE-T Gigabit Ethernet;
- IEEE 802.3ad Link Aggrecation Control Protocol;
- IEEE 802.3ae 10Gbps Ethernet over fiber for LAN;
- IEEE 802.3z Gigabit Ethernet;
- IEEE 802.3an 10GBASE-T 10Gbps Ethernet over copper twisted pair cable;
- IEEE 802.3x Flow Control;
- IEEE 802.1d (STP, GARP, and GVRP);
- IEEE 802.1q/p VLAN;
- IEEE 802.1w Rapid STP;
- IEEE802.1s Multiple STP;
- IEEE 802.1x Port Access Authentication;
- IEEE 802.3af;
- IEEE 802.3at;
- IEEE 802.1ab Link Layer Discovery Protocol;
- IEEE 802.3az Energy Efficient Ethernet;
- RFC 768;
- RFC4330.

2.6. Obsługiwane funkcje bezpieczeństwa:
2.6.1. zapora ogniowa klasy Stateful Inspection;
2.6.2. filtrowanie ruchu na poziomie wartwy aplikacji;
2.6.3. tunelowanie ruchu przez połączenia szyfrowanie IPSec VPN;
2.6.4. ochrona przed malware;
2.6.5. ochrona przed atakami („IPS");
2.6.6. kontrola stron WWW, w tym kontrola certyfikatów stron;
2.6.7. kontrola zawartości poczty e-mail, w tym „antyspam" dla protokołów SMTP;
2.6.8. zarządzanie pasmem, w tym QoS i Traffic shaping;
2.6.9. mechanizmy ochrony przed wyciekiem informacji poufnych;
2.6.10. uwierzytelnianie dwuskładnikowe z wykorzystaniem tokenów sprzętowych lub programowych – wymagane są co najmniej 2 tokeny do uwierzytelniania administratorów i połączeń VPN typu client-to-site;
2.6.11. inspekcja (minimum IPS) ruchu szyfrowanego protokołami SSL/TLS co najmniej dla protokołów HTTP (w tym HTTP/2), SMTP, FTP, POP3;
2.6.12. filtrowanie zapytań DNS w ruchu przechodzącym przez system;

2.6.13. wbudowane mechanizmy automatyzacji (np. obsługa skryptów) po wystąpieniu wybranego zdarzenia – np. zmiana konfiguracji i wysłanie powiadomienia do administratora po wykryciu naruszenia polityki bezpieczeństwa.

2.7. Funkcje firewall IPv4 i IPv6:
- 2.7.1. grupowanie adresów, protokołów, usług sieciowych;
- 2.7.2. rejestrowanie zdarzeń;
- 2.7.3. translacja adresów NAT, PAT, maskarady, ALG („Application Level Gateway" dla SIP);
- 2.7.4. wydzielanie stref bezpieczeństwa („DMZ", „LAN", „WAN");
- 2.7.5. obsługa zewnętrznych repozytoriów z adresami URL oraz adresami IP;
- 2.7.6. filtrowanie ruchu w zależności od kraju, do którego przypisany jest adres IP;
- 2.7.7. uzależnienie reguł od przedziału czasu (dni tygodnia, godziny obowiązywania);
- 2.7.8. integracja z rozwiązaniami SDN przy budowaniu polityk „ACL":
  - Amazon Web Services (AWS);
  - Microsoft Azure;
  - Cisco ACI;
  - Google Cloud Platform (GCP);
  - OpenStack;
  - Vmware NSX;
  - Kubernetes.

2.8. Funkcje VPN:
- 2.8.1. wsparcie dla IKEv1 oraz IKEv2;
- 2.8.2. obsługa protokołu AES z kluczami 128 i 256-bitów w Galois/Counter Mode (GCM);
- 2.8.3. obsługa protokołu Diffie-Hellman grup 19, 20;
- 2.8.4. wsparcie dla topologii Hub and Spoke oraz Mesh;
- 2.8.5. obsługa połączeń Site-to-Site oraz Client-to-Site;
- 2.8.6. monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności;
- 2.8.7. możliwość wyboru tunelu przez protokoły routingu (OSPF, RIP, BGP, trasy statyczne);
- 2.8.8. obsługa uwierzytelniania przez hasło („pre-shared key") i certyfikaty;
- 2.8.9. możliwość ograniczenia liczby jednoczesnych tuneli IPSec;
- 2.8.10. możliwość monitorowania tuneli Site-to-Site i automatycznego aktywowania zapasowego tunelu;
- 2.8.11. obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth;
- 2.8.12. obsługa „Split tunelling" dla połączeń Client-to-Site;
- 2.8.13. możliwość nawiązania połączenia VPN z systemów klasy Windows, Linux, MacOS natywnie (opcjonalnie również przez oprogramowanie klienckie).

2.9. Obsługa łączy WAN:
- 2.9.1. obsługa routingu statycznego i Policy Based Routing (wybór tras routingu w zależności od źródła i protokołów) i dynamicznego: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP, PIM;
- 2.9.2. możliwość filtrowania tras w ramach routingu dynamicznego;
- 2.9.3. obsługa ECMP („Equal cost multi-path") – wybór wielu równoważnych tras;
- 2.9.4. obsługa BFD („Bidirectional Forwarding Detection");
- 2.9.5. obsługa monitorowanie tras w oparciu o stan interfejsu i dostępność adresu IP.

2.10. Obsługa SD-WAN i zarządzanie pasmem:
- 2.10.1. obsługa równoważenia obciążenia („load balancing") do łączy WAN;
- 2.10.2. wsparcie dla SD-WAN dla interfejsów fizycznych i wirtualnych (w tym VLAN i IPSec);
- 2.10.3. określanie maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz obsługa priorytetyzacji ruchu;

2.10.4. możliwość określania pasma indywidualnie dla poszczególnych aplikacji i/lub użytkowników niezależnie od ich adresu IP;
2.10.5. możliwość zarządzania pasmem dla wybranych kategorii URL.
2.11. Ochrona przed malware:
2.11.1. obsługa skanowania ruchu w obu kierunkach także dla protokołów działających na niestandardowych portach (np. FTP na porcie 8080);
2.11.2. obsługa protokołów HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS;
2.11.3. obsługa minimum 200 sygnatur w ramach kontroli aplikacji („L7 firewall"), w tym możliwość definiowania sygnatur ręcznie i pobierania ich z repozytorium;
2.11.4. monitorowanie aplikacji chmurowych, co najmniej: Facebook, Google Docs, Dropbox (pod kątem pobierania i wysyłania plików);
2.11.5. możliwość filtrowania konkretnych protokołów sieciowych wykorzystywanych na danym porcie TCP/UDP;
2.12. Kontrola WWW:
2.12.1. weryfikacja certyfikatów SSL/TLS na stronach;
2.12.2. dostęp do bazy co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne – obsługa filtrowania dostępu wg kategorii;
2.12.3. blokada stron sklasyfikowanych jako niebezpieczne (np.: malware, phishing, spam, dynamic DNS, proxy) i zabronione prawem (np. hazard);
2.12.4. możliwość definiowania wyjątków za pomocą tzw. czarnych i białych list;
2.12.5. obsługa filtrowania stron za pomocą wyrażeń regularnych w adresie URL;
2.12.6. możliwość wyświetlenia ostrzeżenia przed otwarciem określonych stron;
2.12.7. obsługa filtrów „Safe Search" – ochrona przed niechcianymi treściami w wynikach wyszukiwania;
2.12.8. możliwość definiowania komunikatów zwracanych użytkownikowi w określonych sytuacjach;
2.12.9. możliwość wykluczenia inspekcji dla wybranych stron lub reguł.
2.13. Uwierzytelnianie użytkowników w ramach sesji:
2.13.1. obsługa lokalnych kont użytkowników;
2.13.2. obsługa LDAP, RADIUS, RSA SecurID;
2.13.3. obsługa uwierzytelniania wieloskładnikowego;
2.13.4. obsługa uwierzytelniania Single-Sign-On, w tym obsługa integracji z ActiveDirectory, RADIUS, API i SYSLOG;
2.13.5. obsługa uwierzytelniania w oparciu o protokół SAML.
2.14. Zarządzanie:
2.14.1. możliwość konfiguracji przez HTTPS, SSH i platformę centralnego zarządzania i monitorowania;
2.14.2. możliwość zablokowania komunikacji nieszyfrowanej;
2.14.3. możliwość wymuszenia uwierzytelniania dwuskładnikowego;
2.14.4. współpraca z rozwiązaniami monitorowania SNMP (w tym SNMPv2c i SNMPv3), Netflow, sFlow;
2.14.5. możliwość zarządzania przez API, do którego producent udostępnia dokumentację;
2.14.6. wbudowane narzędzia diagnostyczne pozwalające na podgląd sesji, stanu firewall, podgląd pakietów oraz testy połączeń takie jak ping i traceroute;
2.14.7. możliwość aktualizacji szeregu reguł firewall dopiero po ich zatwierdzeniu;
2.14.8. możliwość ograniczenia praw administratorów do określonych części systemu.
2.15. Serwisy zewnętrzne, licencje, gwarancja i wsparcie:

2.15.1. funkcje zewnętrzne (baza sygnatur aplikacji, sygnatury wirusów, sygnatury urządzeń mobilnych, analizy typu Sandbox-Cloud, antyspam, bazy kategorii i reputacji adresów IP oraz DNS itp.), które wymagają licencji subskrypcyjnych powinny być ujęte w ofercie, w tym subskrypcja na 12 lub 36 miesięcy i koszt jej przedłużenia na kolejny okres;

2.15.2. sprzęt jest objęty serwisem gwarancyjnym producenta na co najmniej 5 lat (60 miesięcy) obejmującym naprawę lub wymianę w trybie AHR („advanced hardware replacement") – w ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz całodobowe wsparcie techniczne („24/7").

3. Serwer piaskownicy, serwer do analizy danych, biblioteka dyskowa

3.1. Przeznaczenie (i różnice w specyfikacji):

3.1.1. Serwer piaskownicy

ma umożliwiać odtwarzanie danych, w tym instalację wirtualizatorów, odtwarzanie z kopii zapasowych maszyn wirtualnych, baz danych oraz plików i folderów; serwer ten ma również umożliwić bieżące testowanie procesu data-recovery:

- procesory umożliwiające osiągnięcie wyniku minimum 335*;
- zainstalowane minimum 256GB pamięci RAM;
- 4 wbudowane interfejsy 25Gbps (SFP28);
- 8 wnęk na dyski 2.5", zainstalowane dyski typu hot-plug:
  - 4szt. SSD SATA o pojemności min. 1.92TB;
  - 2szt. M2.NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID1;

3.1.2. Serwer analizy danych

ma umożliwiać bieżącą kontrolę kopii zapasowych, w tym analizę zmian (wykrywanie szyfrowania i anomalii) zapisywanych danych:

- procesory umożliwiające osiągnięcie wyniku minimum 265*;
- zainstalowane minimum 384GB pamięci RAM;
- 2 wbudowane interfejsy 25Gbps (SFP28);
- 12 wnęk na dyski 2.5", zainstalowane dyski typu hot-plug:
  - 8szt. SSD SATA o pojemności min. 1.92TB;
  - 2szt. M2.NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID1;

3.1.3. Biblioteka dyskowa

ma służyć do zapisywania kopii zapasowych na macierzach dyskowych:

- procesory umożliwiające osiągnięcie wyniku minimum 169*;
- zainstalowane minimum 64GB pamięci RAM;
- 4 wbudowane interfejsy 1Gbps (RJ45) – łącznie 6 interfejsów;
- 2-portowa karta 32GB FC (Fiber Channel);
- 8 wnęk na dyski 2.5", zainstalowane dyski typu hot-plug:
  - 2szt. SSD SATA o pojemności min. 480GB;
  - możliwość zainstalowania 2szt. M2.NVMe SSD o pojemności min. 960GB z konfiguracją RAID1;
- system Windows Server 2022 Standard wraz z nośnikiem DVD

***** *wynik w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej*

3.2. Wymagania techniczne:

3.2.1. obudowa zgodna z systemem szaf „rack" o wysokości maksymalnej 1U;

3.2.2. umieszczony na froncie obudowy wyświetlacz/panel LCD pokazujący podstawowe informacje, takie jak adres IPv4 karty zarządzającej, czy status (błędy) systemu;

3.2.3. płyta główna obsługująca 2 procesory 32-rdzeniowe wyprodukowana przez producenta całego serwera i oznaczona jego znakiem firmowym, 16 slotów na pamięć RAM i obsługa co najmniej 1TB pamięci operacyjnej;

3.2.4. zainstalowane 2 procesory minimum 16-rdzeniowe 2.8GHz klasy x86 64-bit dedykowane do pracy z zaoferowanym serwerem;

3.2.5. zainstalowana pamięć DDR5 RDIMM 5600MT/s;

3.2.6. sprzętowy kontroler RAID:
- posiadający 8GB nieulotnej pamięci cache;
- obsługujący RAID: 0, 1, 5, 6, 10, 50, 60;
- wspierający dyski samoszyfrujące;

3.2.7. jeden (1) slot PCIe LP;

3.2.8. wbudowane 2 interfejsy sieciowe 1Gbps (RJ45) oraz interfejsy wymienione wcześniej – porty inne niż FC nie mogą być osiągnięte przez karty w slotach PCIe;

3.2.9. porty zewnętrzne:
- 4szt. USB, w tym 1szt. USB 3.0 z tyłu obudowy i 1szt. microUSB z przodu obudowy;
- 2 porty VGA (DSUB), po jednym z przodu i tyłu obudowy;
- Możliwość rozbudowy o port RS232;

3.2.10. zintegrowana karta graficzna obsługująca rozdzielczość co najmniej 1920x1200;

3.2.11. dwa (2) zasilacze redundantne hot-plug min. 1100W klasy Titanium;

3.2.12. komplet wysuwanych szyn do montażu rack oraz ramię organizer kabli ułatwiających wysuwanie serwera;

3.2.13. dodatkowe zabezpieczenia:
- zatrzask górnej pokrywy i blokada zamykana na klucz;
- możliwość wyłączenia fizycznego przycisku zasilania w BIOS;
- zabezpieczenie BIOS i blokadą zasilania za pomocą hasła;
- czujnik otwarcia obudowy;
- moduł TPM 2.0;
- możliwość dynamicznego włączania portów USB na obudowie bez potrzeby restartu serwera;
- możliwość wymazania danych na dyskach niezależnie od systemu operacyjnego, tj. z poziomu zdalnego zarządzania serwerem;
- ochrona firmware przed manipulacją ze strony złośliwego oprogramowania zgodnie z zaleceniami NIST SP 800-147B i NIST SP 800-155;
- mechanizmy kryptograficzne sprawdzające integralność oprogramowania BIOS (Root of Trust);

3.2.14. karta zdalnego zarządzania wraz z niezbędnymi licencjami:
- możliwość zarządzania niezależnie od włączenia bądź wyłączenia serwera;
- zdalny dostęp WWW do graficznego interfejsu karty zarządzającej;
- zdalne monitorowanie serwera (m.in. prędkości wentylatorów, temperatury);
- szyfrowane połączenie TLS, w tym autoryzacja użytkownika;
- możliwość podmontowania zdalnych napędów wirtualnych;
- wirtualna konsola z dostępem do myszy i klawiatury;
- wsparcie dla IPv6;
- wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
- możliwość konfiguracji wszystkich ustawień (BIOS, RAID itp.) tak, jak lokalnie;
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer oraz zdalnego ustawienia limitu poboru prądu przez konkretny serwer;

- integracja z Active Directory;
- możliwość obsługi przez dwóch (2) administratorów równocześnie;
- wsparcie dla automatycznej rejestracji DNS;
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;
- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;

3.2.15. oprogramowanie do zarządzania:
- możliwość zarządzania serwerami bez udziału dedykowanego agenta;
- możliwość eksportowania raportów o pracy serwera, w tym własnych raportów do plików CSV, HTML, XLS, PDF;
- szybki podgląd stanu środowiska;
- generowanie alertów przy zmianie stanu urządzenia;
- możliwość grupowania urządzeń, definiowania ról administratorów;
- obsługa zdalnego pulpitu (z klawiaturą, myszą i wirtualnymi napędami) podobnie, jak przez interfejs WWW;
- możliwość migracji ustawień między urządzeniami, w tym wirtualnych adresów MAC, WWM, IQN;

3.2.16. wymagane normy i certyfikaty:
- zgodność z normami ISO-9001:2015, ISO-50001 oraz ISO-14001;
- deklaracja elektro-kompatybilności CE;
- zgodność z wymogami dyrektyw WEEE 2002/96/EC (recykling), RE 67/548/EEC (palność) – wymagane pisemne oświadczenie wykonawcy;
- status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022 na liście Windows Server Catalog;

3.2.17. gwarancja:
- możliwość zgłaszania zdarzeń serwisowych 24/7 telefonicznie i przez Internet;
- możliwość pojedynczego kontaktu dla całego rozwiązania producenta, w tym także do sprzedanego oprogramowania;
- możliwość kwalifikowania poziomu ważności naprawy przez zamawiającego;
- naprawa realizowana w siedzibie zamawiającego najpóźniej w następnym dniu roboczym („NBD") od zakończenia diagnostyki przez Certyfikowanego Technika Producenta z właściwym zestawem części do naprawy, chyba że zamawiający zgodzi się na inną formę dla danej naprawy;
- możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii;
- wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta;
- firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

3.3. <u>Dwa deduplikatory</u> wraz z <u>oprogramowaniem do wykonywania kopii zapasowych</u>

3.3.1. oprogramowanie musi umożliwiać:
- realizację backupów:
  - w centrum danych („Data Center");
  - środowisk wirtualnych;
  - ze zdalnych lokalizacji;

- monitorowanie oraz raportowanie środowiska kopii zapasowych;
- zabezpieczenie danych w trybie Continuous Data Protection (CDP) środowisk VMware vSphere;
- zarządzanie synchronizacją realizowaną na poziomie deduplikatorów;
- analizę zreplikowanych danych pod kątem ataku ransomware.

3.3.2. licencja oprogramowania w kontekście backupu, monitoringu i CDP musi:
- obejmować minimum 20 procesorów w serwerach zabezpieczanego środowiska;
- nie posiadać ograniczeń rozmiaru danych, ilości serwerów, baz danych, wykorzystywanych urządzeń taśmowych i dyskowych;
- nie być ograniczona czasowo;

3.3.3. licencja i subskrypcja w kontekście analizy danych musi:
- obejmować wolumen danych o rozmiarze minimum 15TB;

3.3.4. wymagania dotyczące oprogramowania (odczyt i zapis):
- możliwość wyboru miejsca deduplikacji (na źródle lub na medium backupowym) zarówno dla plików, jak i dla baz danych oraz obrazów maszyn wirtualnych;
- możliwość backupu z każdej zabezpieczanej maszyny bezpośrednio na deduplikator (także z deduplikacją na źródle) działający co najmniej na platformach Windows, RedHat, SuSE;
- obsługa backupu blokowego opartego o fizyczne bloki dysków, a nie pliki oraz z możliwością nieindeksowania plików z takiego backupu;
- obsługa inkrementalnego backupu blokowego, który będzie odczytywał tylko te fragmenty dysku, które zmieniły się od ostatniego backupu (mechanizm CBT);
- możliwość łączenia backupu blokowego pełnego i inkrementalnego w jeden pełen backup – łączenie powinno odbywać się na deduplikatorze, wyłącznie na metadanych bez fizycznego odczytu łączonych danych, po połączeniu muszą być dostępne 2 backupy pełne;
- możliwość backupowania pojedynczych plików;
- przechowywanie całości informacji własnych (o backupach, napędach taśmowych, mediach) w centralnym pojedynczym katalogu – skopiowanie tego katalogu na inną maszynę musi pozwolić na uruchomienie na niej serwera backupu identycznego z oryginalnym;
- musi istnieć możliwość wykonania kopii wewnętrznej bazy danych systemu backupu, w trakcie pracy systemu, bez konieczności ograniczania jego funkcjonalności – powinna istnieć możliwość backupu co najmniej na ten sam lub inny deduplikator, urządzenia dyskowe i nośniki taśmowe;
- backup własnej bazy danych musi umożliwiać odtworzenie wszystkich ustawień systemu na zupełnie nowej, świeżo zainstalowanej instancji oprogramowania backupowego;
- obsługa taśm i bibliotek taśmowych, w tym możliwość określania terminu ważności pojedynczej taśmy (zabezpieczenie przed nadpisaniem);
- możliwość automatycznego przyporządkowania taśm wolnych, nieużywanych, nieprzyporządkowanych i / lub przeterminowanych, gdy zabraknie taśm, na których można zapisywać backupy;
- zapisywanie taśm powinno obejmować komplet danych wraz z niezbędnymi opisami (metadanymi), tak, aby włożenie taśmy do innej biblioteki zarządzanej przez zupełnie inną instancję oferowanego oprogramowania pozwalało na pełne odtworzenie danych znajdujących się na tej taśmie;

- utrata wewnętrznych danych oprogramowania backupowego nie może uniemożliwiać odtworzenia jakichkolwiek zbiorów z deduplikatora bądź taśm;
- obsługa łączenia strumieni backupowych z wielu serwerów w sieci LAN równocześnie i bezpośredniego zapisu na napędzie taśmowym (multiplexing);
- zarządzanie bezpośrednią replikacją backupów pomiędzy deduplikatami oferowanego typu z zachowaniem założeń:
  - replikacja realizowana jest na poziomie deduplikatorów (nie oprogramowania);
  - replikacji podlegają wyłącznie te bloki, które nie znajdują się na docelowym deduplikatorze;
  - oprogramowanie przechowuje informacje o wszystkich kopiach danych znajdujących się na deduplikatorach (zarówno źródłowym, jak i docelowym);
- oprogramowanie musi umożliwiać kopiowanie backupów (w obie strony) między dowolnymi mediami, w tym deduplikatorami oferowanego typu, dyskami sieciowymi (CIFS, NFS) oraz nośnikami taśmowymi;
- obsługa backupów systemu plików w trybach: pełnym, różnicowym, przyrostowym (inkrementalnym) – proces odtwarzania niezależnie od rodzaju backupu powinien wyglądać identycznie (zarówno w kontekście zarządzania i wydajności), także dla backupu inkrementalnego połączonego w backup pełny;
- możliwość zatrzymania procesu backupu i jego wznowienia od momentu zatrzymania;
- wsparcie dla krótkotrwałych problemów z siecią (przeciążenia, zaniki, ograniczenia sieci WAN), w tym wsparcie dla deduplikacji i kompresji przesyłanych danych;
- w przypadku nieudanego backupu systemu plików (np. z powodu zerwania łączności) oprogramowanie powinno wznowić backup od ostatnio poprawnie zbackupowanego katalogu lub pliku;
- w przypadku awarii fragmentu taśmy / nośnika oprogramowanie musi umożliwić odtworzenie całości plików, które znajdują się na nieuszkodzonej części nośnika;
- wsparcie dla połączeń: FC, FCoE, iSCSI, NAS, DAS;
- wsparcie dla serwerów plików NAS, w tym integracja z protokołem NDMP;
- wsparcie dla systemów operacyjnych: Windows (także Microsoft Cluster), Linux (RedHat, SuSE, Ubuntu, CentOS);
- wsparcie (moduły producenta oprogramowania) dla aplikacji online: Microsoft Exchange, Microsoft SharePoint;
- wsparcie baz danych: Microsoft SQL Server, Oracle, PostgreSQL, MySQL – możliwość inicjalizacji backupu w oparciu o ilość logów lub inne zdarzenie zdefiniowane przez użytkownika;
- możliwość realizacji kopii zapasowej bazy danych kilkoma (minimum 10) strumieniami jednocześnie;
- możliwość utworzenia i/lub przywrócenia backupu baz MSSQL i Oracle przez ich administratorów bez angażowania administratora rozwiązania backupowego:
  - MSSQL – bezpośrednio z poziomu SQL Server Management Studio;
  - Oracle – w ramach integracji z funkcjonalnością FRA (Fast Recovery Area) za pomocą narzędzia RMAN;
- możliwość odtwarzania systemów operacyjnych bez potrzeby ich ponownej instalacji;
- możliwość odtwarzania na maszynę docelową z poziomu centralnej konsoli systemu backupowego oraz z zabezpieczanego serwera / komputera;

- możliwość wykluczenia z backupu systemu plików wybranych elementów (określonych typów / rozszerzeń plików, folderów, pojedynczych plików);
- integracja konsoli zarządzającej z Active Directory – możliwość przypisywania ról administratorów w oparciu o grupy w domenie;
- możliwość generowania raportów dotyczących zajętości przestrzeni przeznaczonej na składowanie deduplikatów;
- bloki przesyłane z zabezpieczanych serwerów do deduplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym;
- bezprzerwowa dostępność środowiska 24h na dobę przez 7 dni w tygodniu;
- możliwość instalacji prekonfigurowanych agentów jako plików MSI (Windows);

3.3.5. wymagania dotyczące środowisk wirtualnych:

- wsparcie dla środowisk VMware vSphere, VMware ESXI, Microsoft Hyper-V;
- tworzenie i przywracanie backupów bezpośrednio na / z deduplikator;
- możliwość backupu maszyn wirtualnych w trakcie ich normalnej pracy;
- możliwość backupu obrazów całych maszyn wirtualnych;
- możliwość deduplikacji obrazów maszyn (VMDK) z uwzględnieniem zmiennej wielkości bloku danych;
- możliwość odtworzenia całego serwera lub pojedynczych maszyn wirtualnych;
- skalowalność do minimum 2000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu oraz 8000 maszyn w ramach pojedynczego VMware vCenter;
- mechanizm weryfikacji spójności maszyn wirtualnych, w tym możliwość dołączenia własnego skryptu do procesu weryfikacji;
- możliwość utworzenia / przywrócenia kopii przez administratora wirtualizatora;
- możliwość uruchomienia procesu backupowego w VMware przez REST API;
- integracja VMware na poziomie vCenter Plug-in (orchestration, management), vSphere Web Client GUI, vRealize Operations Manager;
- obsługa snapshotów VSS w Hyper-V;
- obsługa ciągłej replikacji RDM w VMware;
- możliwość pominięcia wybranych obrazów dysków w ramach backupu;
- możliwość stworzenia Disaster Recovery całego środowiska wirtualnego, w tym odtwarzanie maszyn na dowolnym wirtualizatorze zgodnym z daną maszyną oraz migrację danych w trybie On-Line na inne zasoby dyskowe;
- wsparcie dla środowisk lokalnych oraz zdalnych w ramach VMware w ramach dostarczonych licencji w następujących trybach:
  - CDP (Continuous Data Protection) – tryb replikacji lokalnej;
  - CRR (Continuous Remote Replication) – tryb replikacji zdalnej;
  - CLR (Continuous Local and Remote Replication) – połączenie CDP oraz CLR;
- brak pojedynczego punktu awarii (Fault-Tolerant) – uszkodzenie pojedynczego elementu nie może uniemożliwić odtworzenia pozostałych (maszyn wirtualnych);

3.3.6. wymagania dotyczące oprogramowania (czasy i harmonogramowanie zadań):

- możliwość tworzenia backupu bazy danych systemu automatycznie oraz wg wyznaczonego harmonogramu;
- włączenie replikacji może następować po zakończeniu backupu oraz zgodnie z kalendarzem;
- możliwość zdefiniowania czasu ważności danych niezależnie dla każdego nośnika w momencie definiowania zadania deduplikacji/kopiowania – zarówno przez GUI, jak i przez wiersz poleceń;

- możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata) – po okresie ważności backupy muszą być automatycznie usunięte;
- ochrona ostatniego (najnowszego) backupu przed modyfikacją i usunięciem;

3.3.7. oferowane rozwiązanie musi umożliwiać:
- bieżące testy weryfikacyjne całego zabezpieczenia;
- tworzenie do 500 snapshotów danych po synchronizacji deduplikatorów;
- ręczne tworzenie blokad na wybranych danych (kopiach);
- skanowanie i analizę metadanych i pełnej zawartości pod kątem ataków ransomware (zarówno: pojedynczych plików, baz danych, dysków wirtualnych), wsparcie dla analizy backupów blokowych co najmniej dla systemu Windows;
- rejestrowanie analizy danych w formie logów zdarzeń (Event Log);
- możliwość analizowania danych backupowych na wolumenie minimum 15TB FET;

3.3.8. wymagane metody analizy danych pod kątem ataków ransomware:
- silne szyfrowanie z oryginalną nazwą pliku;
- częściowe silne szyfrowanie z oryginalną nazwą pliku;
- silne szyfrowanie RMS/MS_EFS;
- silne szyfrowanie z nowym znanym rozszerzeniem;
- częściowe silne szyfrowanie z nowym znanym rozszerzeniem;
- silne szyfrowanie z zaciemnioną nazwą pliku;
- szyfrowanie strony bazy danych;
- nowe rozszerzenie pliku;
- ukrycie nazwy pliku;
- słabe szyfrowanie z nowym rozszerzeniem pliku;
- słabe szyfrowanie z oryginalną nazwą pliku;
- częściowe szyfrowanie z zaciemnioną nazwą pliku;
- szyfrowanie wewnątrz z oryginalną nazwą pliku;
- częściowo słabe szyfrowanie z oryginalną nazwą pliku i typem pliku;
- słabe szyfrowanie z zaciemnioną nazwą pliku;
- archiwum grupowe utrzymujące wymazaną oryginalną nazwę pliku;
- silne szyfrowanie z nowym znanym rozszerzeniem — usuwanie zduplikowanych plików;
- wypełnienie zerami z nowym znanym rozszerzeniem;
- wypełnienie zerowami z oryginalną nazwą pliku;
- wypełnienie zerami z zaciemnioną nazwą pliku;

3.3.9. wymagania sprzętowe odnośnie deduplikatorów:
- 48TB przestrzeni użytkowej netto;
- skalowalność przestrzeni deduplikatów do minimum 170TB netto;
- możliwość rozbudowy o warstwę chmury (Cloud) do długotrwałego przechowywania danych (Long Term Retention) bez pośrednictwa dodatkowych urządzeń (Gateway) – wymagane wsparcie dla Amazon Web Services, Microsoft Azure, Google GCP – wymagane szyfrowanie danych oraz dostarczenie licencji na minimum 200TB przestrzeni netto dla warstwy chmurowej;
- 8 portów optycznych 10Gbps (wraz z wkładkami), obsługa protokołów CIFS, NFS oraz deduplikacji na źródle na każdym z portów;
- 2 porty FC 16Gbps, obsługa protokołów VTL oraz deduplikacji na źródle;

- wolny slot HBA na dodatkową kartę z 2 portami FC, w tym oficjalne wsparcie takiej konfiguracji przez producenta urządzenia oraz możliwość natychmiastowego zamówienia u producenta wymaganej karty rozszerzeń;
- możliwość jednoczesnego obsługiwania protokołów CIFS i NFS, deduplikacji na źródle (ze wsparciem dla oferowanej aplikacji backupowej), protokołów VTP (minimum 10 jednoczesnych połączeń);
- licencje wieczyste dla wszystkich protokołów oraz maksymalnej pojemności urządzenia (o ile są potrzebne);
- możliwość jednoczesnej obsługi 250 strumieni, w tym 150 zapisu, 50 odczytu i 50 replikacji – niezależnie od protokołów, interfejsów i serwerów / agentów źródłowych;
- wsparcie dla bibliotek taśmowych StorageTek L180 i IBM TS 3500 oraz technologii LTO5 i LTO7;
- możliwość emulacji (w przypadku VTL'a) minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów;
- obsługa asynchronicznej replikacji w trybach 1:1, wiele:1, 1:wielu i kaskadowym (np. A do B, B do C…);
- poprawne działanie przy zapełnieniu 90% bieżącej pojemności;
- ochrona danych w oparciu o RAID6 lub technologię równoważną;
- obsługa blokad nadpisania / usuwania danych (WORM) w trybie niezdejmowalnym (Compliance) oraz zdejmowalnym, w tym niezbędne licencje wieczyste;
- Compliance zgodny z normami w zakresie ochrony danych: SEC 17a-4(f), CFTC Rule 1.31b, FDA 21 CFR Part 11, Sarbanes-Oxley Act, IRS 98025 and 97-22, ISO Standard 15489-1, MoREQ2010.

4. Dodatkowe wymagania dotyczące całości systemu:
   4.1. Wykonawca zapewni obsługę gwarancyjną całego systemu na okres nie krótszy niż 5 lat licząc od daty dokonania odbioru końcowego bez zastrzeżeń – dopuszczalne jest, że w ramach tej gwarancji wykonawca wykupi na własny koszt usługi serwisowe u producenta rozwiązania.
5. W ramach oferty należy uwzględnić:
   5.1. wdrożenie dostarczonego sprzętu;
   5.2. przeszkolenie z zakresu maszyn wirtualnych i fizycznych;
   5.3. przeszkolenie z zakresu procesu weryfikacji kopii i odzyskiwania systemu;
   5.4. wsparcie powdrożeniowe przez okres 12 miesięcy.