**Numer sprawy: 17/2024 Załącznik nr 1 do SWZ / Załącznik nr 1 do Umowy**

**OPIS PRZEDMIOTU ZAMÓWIENIA – zwany OPZ**

**I. Przedmiot zamówienia.**

1. Przedmiotem zamówienia jest **Dostawa oprogramowania komputerowego dla Urzędu Pracy m.st. Warszawy.**
2. Definicje OPZ:
3. **Wykonawca** – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej.
4. **Zamawiający** – Miasto st. Warszawa – Urząd Pracy m.st. Warszawy.
5. **Opiekun ze strony Zamawiającego lub Opiekun ze strony Wykonawcy,** zwany również Opiekunem – osoba upoważniona do kontaktów, wskazana w umowie.
6. **Wada** – cecha oprogramowania obniżająca właściwości funkcjonalne, objawiająca się poprzez brak pewnych funkcji, niższą wydajność lub niższą niezawodność pracy w porównaniu z oprogramowaniem pozbawionym wady. Wada może powodować utratę lub uszkodzenie danych. Za wadę uznaje się również niespełnianie przez oprogramowanie wymagań określonych w pkt III. OPZ – Warunki szczegółowe. Za wadę uznaje się również brak legalności dostarczonych licencji do oprogramowania ocenianą na podstawie możliwości weryfikacji zapewnianych przez producenta danego oprogramowania.
7. Zapotrzebowanie na oprogramowanie zostało opisane w pkt III. OPZ - Warunki szczegółowe.

**II. Warunki realizacji umowy** – Wymagania ogólne.

1. Wykonawca, co najmniej na 1 dzień przed planowaną dostawą, poinformuje Opiekuna ze strony Zamawiającego o terminie dostawy oprogramowania.
2. Dostawa/y oprogramowania realizowana/e będzie/będą do siedziby Urzędu Pracy m.st. Warszawy przy ul. Grochowskiej 171B w Warszawie. Oprogramowanie, gdzie producent przewiduje jedynie jego postać elektroniczną, Wykonawca dostarczy w postaci elektronicznej lub spowoduje, aby producent oprogramowania przesłał je do Opiekuna ze strony Zamawiającego na wskazany adres poczty elektronicznej, niezwłocznie po udzieleniu licencji na oprogramowanie lub po dokonaniu aktywacji przedłużenia wsparcia oprogramowania.
3. Wykonawca zrealizuje przedmiot zamówienia w ramach wynagrodzenia określonego w umowie, w terminie określonym w umowie. Dostawy oprogramowania w postaci fizycznej realizowane będą w dni robocze, w godzinach 8:00 – 15:45.
4. Wykonawca dostarczy oprogramowanie spełniające wszystkie wymagania dotyczące bezpieczeństwa, określone w obowiązującym w Polsce prawie.
5. Zaoferowane oprogramowanie musi być ogólnodostępne na rynku oraz musi być w najnowszej wersji dostępnej na rynku na dzień składania ofert.
6. Oprogramowanie musi pochodzić z autoryzowanego kanału sprzedaży producenta i musi być dostarczone w formie licencji na warunkach producenta. Przedłużenie wsparcia na oprogramowanie musi pochodzić z autoryzowanego kanału sprzedaży producenta i musi być dostarczone na warunkach producenta oprogramowania.
7. Zamawiający wymaga dostarczenia oprogramowania przeznaczonego do użytkowania przez podmioty komercyjne lub instytucje rządowe i samorządowe, ponieważ Zamawiający jest jednostką samorządową. Oprogramowanie należy dostarczyć w formie przewidzianej przez producenta oprogramowania (np. nośniki magnetyczne/optyczne/elektroniczne, licencje papierowe, klucze dostępu, linki umożliwiające pobranie oprogramowania, zapisy na portalu licencyjnym producenta).
8. Okres użytkowania oprogramowania wyszczególnionego w pkt III. OPZ musi być bezterminowy, z wyłączeniem przypadków opisanych jako terminowe. Zaoferowane oprogramowanie musi być licencjonowane w formie licencji grupowych lub licencji pudełkowych, o ile nie określono innego typu licencjonowania w pkt III. OPZ.
9. Wykonawca odpowiada za wszelkie wady prawne dostarczonego oprogramowania i licencji, w tym również za ewentualne roszczenia osób trzecich wynikające z naruszenia przez Zamawiającego w związku z eksploatacją dostarczonego oprogramowania praw własności intelektualnej lub przemysłowej, w tym praw autorskich, patentów, praw ochronnych na znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe. Ewentualne roszczenia osób trzecich wynikające z praw autorskich lub patentowych, dotyczące przedmiotu dostawy, będą dochodzone bezpośrednio od Wykonawcy.
   1. **Warunki szczegółowe:**
      * 1. **Oprogramowanie komputerowe wchodzące w zakres zamówienia gwarantowanego:**

|  |  |  |
| --- | --- | --- |
| **Poz. 1. Oprogramowanie antywirusowe** | | **Ilość – 1 komplet** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania:**  Aktualizacja/odnowienie subskrypcji pakietu oprogramowania ESET Protect Enterprise On-prem dla 400 stacji roboczych, urządzeń mobilnych i serwerów, w tym liczba chronionych serwerów nie przekroczy 40.  Lub oprogramowanie równoważne o podobnej funkcjonalności w wersji On-prem spełniające w szczególności poniższe wymagania:  Liczba stacji roboczych i laptopów opartych na systemie Windows i urządzeń mobilnych opartych na systemie Android objętych licencją: co najmniej 360 szt.  Liczba serwerów opartych na systemie Windows i Linux objętych licencją: co najmniej 40 szt. (ochrona w zakresie plików udostępnianych klientom, lokalna ochrona systemu operacyjnego serwera).  W ramach licencji, możliwość instalacji na zasobach Zamawiającego minimum 1 serwera do zarządzania oraz minimum 3 serwerów proxy, do minimalizowania ruchu sieciowego systemu antywirusowego pomiędzy lokalizacjami lub innego rozwiązania typu proxy, zapewniającego minimalizację ruchu sieciowego pomiędzy trzema lokalizacjami, do lokalnego serwera zarządzania i do Internetu.  W ramach modułu antywirusowego oprogramowania równoważnego dla stacji roboczych i serwerów plików wymagane są funkcjonalności:  Pełna ochrona przed oprogramowaniem typu: wirusy komputerowe, zagrożenia szyfrujące ransomware, robaki, programy szpiegujące i inne zagrożenia.  Wykrywanie i usuwanie niebezpiecznego oprogramowania typu: adware, spyware, dialer, phishing, narzędzia hakerskie, backdor, rootkit.  Wykrywanie i blokowane aktywności botnetów, funkcja blokowania Exploit’ów.  Wykrywanie zagrożeń w czasie rzeczywistym, skanowanie plików na żądanie użytkownika, skanowanie zgodnie z harmonogramem lub w trakcie nieaktywności użytkownika.  Ochrona plików, a dla stacji roboczej pracującej pod kontrolą Windows również poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programów pocztowych, co najmniej MS Outlook - ochrona realizowana za pomocą automatycznej integracji odpowiednich modułów z programem pocztowym, bez konieczności dodatkowej konfiguracji, wraz z funkcją automatycznej zmiany rozszerzeń potencjalnie niebezpiecznych załączników lub blokowania niebezpiecznych załączników.  Zatrzymywanie ataków bezplikowych za pomocą algorytmów wykrywających zmienione lub przejęte aplikacje, podejrzane procesy rezydujące w pamięci.  Ochrona w czasie rzeczywistym ruchu HTTP, HTTPS na poziomie stacji roboczej. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. Ochrona realizowana za pomocą automatycznej integracji odpowiednich modułów z przeglądarką internetową, bez konieczności dodatkowej konfiguracji wraz z możliwością definiowania odpowiednich wykluczeń.  Ochrona przed atakiem z sieci polegająca na wykrywaniu znanych luk w oprogramowaniu i blokowaniu prób wykorzystania tych luk.  Ochrona przed botnetami polegająca na wykrywaniu złośliwej komunikacji wykorzystywanej przez sieci botnet wraz z identyfikacją procesów które taka komunikacje próbują realizować.  Małe obciążenie pracą oprogramowania antywirusowego, minimum w zakresie zajętości pamięci RAM i wykorzystania procesora.  Wykorzystanie do ochrony zarówno sposobów konwencjonalnych jak i technik opartych na uczeniu maszynowym.  Wykorzystanie systemu HIPS przy ochronie stacji i serwerów pracujących pod kontrolą Windows.  Wykorzystywanie systemu ochrony w chmurze, gdzie próbki są przesyłane na serwery producenta i tam poddawane szczegółowej analizie w tym próbki muszą być uruchamiane. Przy czym musi istnieć możliwość zdefiniowania typów plików które będą wyłączone z procesu przesyłania do chmury producenta. Wymaga się aby oprogramowanie miało możliwość wykluczenia z wysyłki do chmury minimum archiwów i dokumentów MS Office. Opcja musi być możliwa do zdefiniowania z poziomu konsoli centralnego zarządzania. Ponadto na konsoli do zarządzania musi być dostępna informacja na temat plików przesyłanych do chmury w celu ich analizy.  Możliwość blokowania dla stacji roboczych pracujących pod kontrolą Windows co najmniej zewnętrznych nośników danych (pendrive), nośników optycznych.  Możliwość definiowania, z poziomu konsoli centralnego zarządzania, polis dla ochrony czasu rzeczywistego i skanowania plików, dla poszczególnych grup komputerów, zawierająca co najmniej ustawienia: lista skanowanych napędów (wszystkie napędy lokalne, wszystkie napędy wymienne (nośniki wymienne), wszystkie napędy sieciowe, itp.), sposób identyfikacji plików (wszystkie pliki, bazujący na rozszerzeniach, itp.), załączenie/wyłączenie skanowania archiwów określenie maksymalnej wielkości skanowania archiwów i głębokości skanowania, określenie zachowania w przypadku archiwów szyfrowanych, definicja wykluczeń ze skanowania, tryb pracy oprogramowania antywirusowego (skanowanie przy dostępie do pliku, skanowanie przy wykonaniu pliku, skanowanie przy dostępie nośnika wymiennego itp.) osobno definiowany poziom skanowania dla raportowania i ochrony, tak aby przy najwyżej czułości oprogramowania pojawiały się stosowne raporty pomimo możliwości wystąpienia zwiększonej ilości tzw. „fałszywych pozytywów” .  Możliwość definiowania dla stacji roboczych, z poziomu konsoli centralnego zarządzania, polis dla ochrony poczty przychodzącej i wychodzącej, dla poszczególnych grup komputerów, zawierająca co najmniej ustawienia: skanowanie załączników w zakresie załącz/wyłącz oraz określenie maksymalnego rozmiaru skanowanych archiwów, ochrona przed potencjalnie niebezpiecznymi załącznikami w zakresie usuwania ich z emaila lub/i zmiany rozszerzenia wraz z możliwością zdefiniowania rozszerzeń potencjalnie niebezpiecznych załączników (moduł antywirusowy integrujący się z programami do obsługi poczty minimum z MS Outlook).  Możliwość definiowania dla stacji roboczych, z poziomu konsoli centralnego zarządzania, polis dla ochrony HTTP i HTTPS, dla poszczególnych grup komputerów, zawierająca co najmniej ustawienia: definicja poziomu skanowania heurystycznego w zakresie załącz/wyłącz oraz poziom skanowania heurystycznego, załączenie/wyłączenie funkcji sprawdzających, czy adres nie jest zawarty w bazie danych potencjalnie niebezpiecznych stron, definicja wykluczeń - listy adresów IP i URL, które mają nie podlegać sprawdzaniu, definicja wykluczeń – lista certyfikatów stron HTTPS zabronionych, dozwolonych, niepodlegających kontroli.  Możliwość definiowania, z poziomu konsoli centralnego zarządzania, polis dla poszczególnych grup komputerów, definiująca załączenie/wyłączenie poszczególnych modułów oprogramowania (skanowanie antywirusowe, skanowanie poczty email, skanowanie stron WWW, moduł firewall).  Możliwość zablokowania, z konsoli centralnego zarządzania, modyfikacji ustawień oprogramowania antywirusowego przez użytkownika zalogowanego na stacji roboczej.  Możliwość zdefiniowania hasła umożliwiającego odinstalowanie zainstalowanego na stacji roboczej oprogramowania antywirusowego i zabezpieczającego oprogramowanie przed samowolnym jego odinstalowaniem przez użytkownika.  Obsługa statycznych i dynamicznych grup, do których konsola centralnego zarządzania dodaje poszczególne stacje robocze na podstawie ich specyficznych cech i przypisywanie im odpowiednich polis.  Cykliczna aktualizacja oprogramowania antywirusowego z możliwością pobierania aktualizacji z serwerów producenta oprogramowania oraz z serwerów do centralnego zarządzania i wewnętrznych serwerów proxy, aktualizacja inicjowana według harmonogramu oraz na żądanie. Producent oprogramowania musi publikować aktualizacje baz sygnatur co najmniej kilka razy dziennie a aktualizacja musi działać w trybie przyrostowym.  Możliwość, z poziomu konsoli centralnego zarządzania, uzyskania szczegółowej informacji o stanie zabezpieczenia poszczególnych stacji roboczych i serwerów w zakresie terminu ostatniej aktualizacji baz sygnatur, ostatniego pełnego skanowania, ostatniej aktualizacji danych, informacji o wykrytych zagrożeniach (zawirusowanych plikach, mailach, stronach internetowych, które użytkownik próbował otwierać) wraz z automatycznym wyróżnianiem na konsoli urządzeń, które od pewnego czasu nie komunikowały się z serwerem centralnego zarządzania lub mają nieaktualne bazy sygnatur.  Możliwość, z poziomu konsoli centralnego zarządzania, ręcznego inicjowania zadań aktualizacji, skanowania plików dla poszczególnych stacji roboczych.  Moduł skanujący musi pochodzić od innego producenta, niż moduł skanujący wykorzystywany przez Zamawiającego do ochrony poczty elektronicznej oparty na rozwiązaniu Forti Mail.  W ramach modułu firewall oprogramowania równoważnego dla stacji roboczych Windows wymagane są funkcjonalności:  Możliwość, z poziomu konsoli centralnego zarządzania definiowania reguł wbudowanego w oprogramowanie do ochrony stacji roboczych modułu firewalla w zakresie trybu pracy (automatyczny – gdy wszystkie nowe połączenia przychodzące są blokowane a zezwolone są wszystkie połączenia wychodzące, interaktywny – gdy jeśli dany ruch sieciowy nie jest wymieniony w regułach wówczas oprogramowanie wyświetla użytkownikowi odpowiednie pytanie/alert, oparty na regułach – gdy na konsoli centralnego zarządzania wskazuje się reguły ruchu sieciowego, uczenia się – gdy system automatycznie tworzy i zapisuje reguły na podstawie zdefiniowanych w konsoli centralnego zarządzania zasad). Z poziomu konsoli centralnego zarządzania musi być możliwość osobnego zdefiniowania poza regułami zasad działania modułu firewalla, zasady w zakresie zezwolenia lub blokady na: udostępnianie plików i drukarek, użycie protokołu UPNP, zezwolenie na połączenia przychodzące: RPC, pulpitu zdalnego, ponadto na logowanie do grup multicast za pośrednictwem IGMP, komunikację zmostkowanych połączeń, używanie protokołu odnajdywania usług w sieci WEB, rozwiązywanie adresów multicast, obsługa grupy domowej Windows. Ponadto wbudowany w oprogramowanie moduł firewalla musi zapewniać możliwość wskazania znanych sieci za pomocą między innymi wskazania nazwy przyrostka DNS, adresu IP: Serwera Wins, DNS, DHCP, bramy sieciowej oraz typu karty sieciowej, identyfikatora SSID, typu zabezpieczania i typu szyfrowania sieci WLAN. Możliwość tworzenia wielu profili dla zapory i przypisywania tych profili do kart sieciowych. Wykrywanie modyfikacji aplikacji (gdy reguły bazują na dopuszczaniu ruchu sieciowego generowanego przez daną aplikację).  Możliwość użycia przez użytkownika na stacji roboczej wbudowanej tzw. bezpiecznej przeglądarki internetowej. Praca w bezpiecznej przeglądarce musi być sygnalizowana po przez kolor oraz informacje na ramce przeglądarki.  Możliwość filtrowania adresów URL w oparciu o co najmniej 100 kategorii i podkategorii na podstawie reguł zdefiniowanych z poziomu konsoli centralnego zarządzania.  Dla urządzeń przenośnych oprogramowania równoważnego wymagane są funkcjonalności:  Ochrona antywirusowa urządzeń mobilnych wykorzystujących oprogramowanie minimum Android. W zakresie skanowania wszystkich plików zarówno w pamięci wewnętrznej jak i na karcie SD. Skanowanie musi być możliwe do przeprowadzenia minimum w 2 trybach – inteligentnym i dokładnym. Skanowanie powinno być przeprowadzane automatycznie w czasie gdy urządzenie jest w trybie bezczynności, podłączone do ładowarki.  Możliwość wskazania zaufanej karty SIM.  Możliwość zarządzania urządzeniami mobilnymi wykorzystującymi oprogramowanie minimum Android za pomocą funkcji typu MDM w zakresie: usunięcia zawartości urządzenia, przywrócenia ustawień fabrycznych, zablokowania urządzenia, uruchomienia sygnału dźwiękowego, lokalizację GPS, listy zainstalowanych aplikacji, możliwość blokowania aplikacji po: nazwie, aplikacji/pakietu, uprawnienia aplikacji, pochodzące z nieznanego źródła.  W zakresie funkcji EDR oprogramowania równoważnego wymagane są funkcjonalności:  Zapewnienie zintegrowanego modułu klasy EDR posiadającego na stacjach roboczych i serwerach minimum Windows funkcjonalność monitorowania aktywności komputera w sieci Zamawiającego w czasie rzeczywistym, analizę podejrzanych procesów, natychmiastową reakcję na incydenty i ataki w postaci generowania alertów oraz monitorowanie zdarzeń jakie procesy/programy generują podczas pracy, logowanie tych zdarzeń zapewniające możliwość prześledzenia na konsoli do zarządzania jakie działania w systemie wykonał dany proces/program.  Moduł kasy EDR do swojej pracy musi wykorzystywać i współpracować z modułem antywirusowym uruchomionym na komputerze.  Moduł kasy EDR musi posiadać minimum 800 wbudowanych reguł wykrywania zapewnianych i aktualizowanych przez producenta systemu po wystąpieniu których nastąpi wyzwolenie alarmu bezpieczeństwa, wraz z możliwością tworzenia własnych reguł i edycji reguł dostarczanych przez producenta rozwiązania.  Moduł kasy EDR musi porównywać wykrywane anomalnie z bazą MITRE Adversarial Tactics, Techniques, and Common Knowledge oraz zapewniać dostęp do kompleksowych informacji o zagrożeniach.  Na konsoli zarządzania modułu EDR musi być możliwość: łatwego edytowania reguł wykrywania w tym za pomocą plików xml, zmiany czułości reguł detekcji dla różnych grup komputerów aby dostosować czułość do danego profilu pracy użytkowników, wskazania wykluczenia dotyczącego procesu lub procesu „rodzica”, zdefiniowania wykluczenia musi automatycznie rozwiązywać alarmy pasujące do danego wykluczenia, kryteria wykluczeń muszą być tworzone co najmniej w oparciu o: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, skrót minimum SHA-1, nazwę komputera, grupę, użytkownika; blokowania plików po sumach kontrolnych wraz z określeniem akcji jaka ma być wykonana po wykryciu próby uruchomienia takiego pliku.  Na konsoli zarządzania modułu EDR administrator musi mieć możliwość: oznaczania plików wykonywalnych, bibliotek DLL jako bezpieczne zaś skryptów jako bezpieczne lub niebezpieczne oraz możliwość pobrania plików do analizy i zablokowania, dokonania weryfikacji uruchomianych plików wykonywalnych na chronionej stacji roboczej w zakresie skrótu minimum SHA-1, typu podpisu, wydawcy, opis pliku, wersja pliku, nazwa firmy/produktu, wersja produktu, oryginalna nazwa pliku, rozmiar pliku, reputacja, popularność pliku. Konsola musi również zapewniać możliwość dodawania komentarzy, tagów, nadawania nazw regułom oraz możliwość podłączenia się do stacji roboczej i wykonania poleceń powershell.  Na konsoli zarządzania modułu EDR administrator musi mieć możliwość: weryfikacji uruchomionych plików wykonywalnych i skryptów na chronionej stacji roboczej, minimum w zakresie drzewa procesów, modyfikacji plików i rejestru, zestawionych połączeń sieciowych, utworzonych plików wykonywalnych. W przypadku skryptów dodatkowo muszą być widoczne parametry uruchomienia i wykaz wykonanych przez skrypt czynności.  Na konsoli zarządzania modułu EDR administrator musi mieć możliwość: obserwacji szczegółowych informacji na temat wykrytych zagrożeń. Ponadto na konsoli zarzadzania musi być możliwość wykrywania oprócz aktualnych zagrożeń również zagrożeń historycznych na podstawie nowo utworzonej reguły lub np. zaktualizowanych reguł istniejących aby odszukać wszystkie komputery na których takie zagrożenie w przeszłości się pojawiło – uruchomienie przetwarzania reguł w oparciu o dane historyczne.  System EDR musi zapewniać zsynchronizowaną reakcje obronną w każdym chronionym elemencie sieci w tym izolacje komputera od sieci LAN.  System EDR musi minimum wysyłać zaistniałe, wykryte zdarzenia do konsoli centralnego zarządzania oprogramowaniem antywirusowym aby w jednym miejscu były widocznie wszystkie zdarzenia dotyczące danego komputera.  Serwer systemu EDR musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych minimum w zakresie MS SQL, MySQL oraz mieć możliwość instalacji na minimum na systemach Windows Server minimum 2016. Dopuszcza się również wsparcie dla instalacji serwera/serwerów systemu EDR w postaci maszyny wirtualnej wspierającej uruchomienie w środowisku vMware opartej na systemie Linux i bazie danych MySQL, Postgresql również w zakresie pracy wieloserwerowej rozproszonej bez konieczności zakupu dodatkowych licencji.  Agent systemu EDR musi umożliwić instalację minimum na systemach Windows 10/11 Windows Server, współpracować z modułem antywirusowym, zapewniać powiadomienia dla użytkownika w przypadku zadziałania reguł administracyjnych w zakresie blokowania/usuwania plików, połączenie między agentem a serwerem EDR musi być szyfrowane.  W zakresie funkcji szyfrowanie dysków stacji roboczych oprogramowania równoważnego wymagane są funkcjonalności:  Obsługa szyfrowania danych na dyskach na komputerach obsługiwanych przez system operacyjny minimum Windows 10/11 w 32 i 64-bitowej wersji.  Autentykacja typu Pre-boot tj. uwierzytelnianie użytkownika zanim zostanie uruchomiony system operacyjny z możliwością czasowego lub całkowitego wyłączenia uwierzytelniania pre-boot z poziomu serwera zarządzania.  Wykorzystanie do szyfrowania modułu TPM, technologii TCG OPAL, szyfrowanie danych na komputerach z UEFI.  Interfejs użytkownika minimum w języku polskim i angielskim.  Zarządzanie funkcjonalnością szyfrowania z konsoli centralnego zarządzania.  Funkcja odzyskiwania dostępu do danych w przypadku utraty hasła przez użytkownika poprzez użycie otrzymanego od administratora jednorazowego hasła wygenerowanego z poziomu konsoli centralnego zarządzania. Funkcja dysku ratunkowego generowanego z konsoli centralnego zarządzania dla każdego zaszyfrowanego i zarządzanego komputera.  Możliwość definiowania z poziomu konsoli centralnego zarządzania wymaganej złożoności hasła użytkownika do autentykacji pre-boot minimum w zakresie minimalnej liczby znaków, złożoności hasła w zakresie wymagania użycia małych/dużych liter cyfr, znaków specjalnych. Ponadto definicja okresu ważności, ilości nieudanych logowań po których pre-boot się blokuje, blokada możliwości zmiany hasła.  Możliwość ograniczenia z poziomu konsoli centralnego zarządzania wyświetlania interfejsu graficznego użytkownikom oraz możliwość zablokowania dostępu do zaszyfrowanego dysku.  W zakresie funkcji sandbox w chmurze producenta oprogramowania równoważnego wymagane są funkcjonalności:  Ochrona przed zagrożeniami 0-day, do działania wykorzystuje chmurę producenta rozwiązania.  Automatyczne podejmowanie decyzji przez system czy dana próbka ma być przesłana do analizy.  Możliwość ręcznego wskazania próbek, które mają być przeanalizowane przez system.  Możliwość definiowania na konsoli centralnego zarządzania ustawień dla typów plików jakie mają zostać przesłane automatycznie do chmury minimum w zakresie: archiwa, skrypty, możliwy spam, dokumenty, pliki typu .jar, .reg, .msi wraz z określeniem czasu przechowywania plików w chmurze producenta, maksymalnego rozmiaru przesyłanych plików, wskazania wykluczeń z przesyłania za pomocą nazw i folderów przechowywania. Po zakończonej analizie wyniki muszą być przesłane do modułu źródłowego z którego pochodzi dany plik.  Na konsoli centralnego zarządzania musi istnieć możliwość sprawdzenia listy plików przekazanych do analizy wraz z ich statusami i wynikami sprawdzania. Analiza plików musi się zakończyć jednym z wymienionych statusów: czysty/podejrzany/bardzo podejrzany/szkodliwy lub równoważne.  W przypadku stacji roboczych musi istnieć możliwość konfiguracji systemu na konsoli centralnego zarządzania tak aby do czasu zakończenia analizy wstrzymana była możliwość uruchamiania plików (pobranych przez przeglądarkę, wyodrębnionych z archiwów, uruchamianych z nośników wymiennych, zapisanych z maili).  W ramach serwera zarządzania oprogramowania równoważnego realizującego funkcje konsoli centralnego zarządzania ponadto wymagane są funkcjonalności:  Serwer zarządzania musi być dostępny w wersji on-prem. Możliwy do zainstalowania na serwerze wykorzystujących system Windows Server i Linux oraz bazę danych minimum MS SQL i MySQL, a także w postaci obrazu ova do uruchomienia serwera w postaci osobnej maszyny wirtualnej w środowisku vMware. Bez konieczności zakupu dodatkowych licencji.  Serwer zarzadzania musi zapewniać interfejs dla administratora w języku minimum polskim i angielskim – do wyboru w momencie logowania. Nie dopuszcza się wyboru w momencie instalacji. Konsola centralnego zarządzania musi umożliwić w jednym miejscu zarządzanie wszystkimi funkcjami. Dopuszcza się wyjątek dla funkcjonalności EDR, gdzie ta funkcjonalność może posiadać osobny serwer zarządzania spełniający wymagania określone w pkt 45, jednak serwery musza się komunikować ze sobą. Dostęp do interfejsu/konsoli zarzadzania musi być zapewniony z wykorzystaniem protokołu https i przeglądarki internetowej.  Serwer zarządzania musi zapewniać możliwość utworzenia własnego CA oraz możliwość generowania potrzebnych certyfikatów do szyfrowania połączeń pomiędzy poszczególnymi modułami systemu ochrony.  Serwer/konsola centralnego zarządzania musi zapewniać zbieranie podstawowych danych na temat podzespołów zainstalowanych w chronionych urządzeniach (procesor, pamięć RAM, informacje o twardych dyskach, pamięci masowej, drukarki, karty sieciowe, informacje o systemie operacyjnym, informacje o modułach zainstalowanych w ramach systemu ochrony itp.).  Serwer/konsola centralnego zarządzania musi zapewniać możliwość zdalnej instalacji i deinstalacji oprogramowania firm trzecich na stacjach roboczych, wykrywania sklonowanych komputerów na podstawie unikalnego identyfikatora sprzętowego, wykrywanie niezarządzanych komputerów w sieci.  Serwer/konsola centralnego zarządzania musi zapewniać możliwość utworzenia dodatkowych kont administracyjnych do zarządzania systemem zarówno lokalnych jak i umożliwić integracje z Active Directory wraz z możliwością wymuszenia dwuetapowej autoryzacji podczas logowania się do konsoli. Dodatkowe konta muszą mieć możliwość zdefiniowania zakresu uprawnień w zakresie ograniczenia zarzadzania do określonych polityk, grup statycznych, dynamicznych, zarządzania licencjami, zadaniami administracyjnymi co najmniej w zakresie odczyt, użyj, modyfikacja, brak. Możliwość konfiguracji czasu bezczynności, po którym następuje automatyczne wylogowanie.  Serwer/konsola centralnego zarządzania musi zapewniać współprace z agentami gdy następuje czasowa utrata połączenia. W takim przypadku agent musi przechowywać ostatnią konfiguracje i realizować ochronę komputera wg. zapisanych zasad a po ponownym nawiązaniu połączenia dokonać aktualizacji i przesłać logi.  Serwer/konsola centralnego zarządzania musi posiadać minimum 50 różnych szablonów raportów zdefiniowanych przez producenta oprogramowania równoważnego oraz umożliwiać tworzenie własnych raportów przez administratora systemu z możliwością wyboru formy wizualizacji: tabelaryczna, wykres (kołowy, pierścieniowy, liniowy, słupkowy, punktowy), oba elementy jednocześnie. Wraz z możliwością importu i eksportu zdefiniowanych szablonów raportu.  Cykliczne generowanie raportów zgodnie z harmonogramem i dostarczanie ich na zdefiniowane adresy email administratorów oraz generowanie raportów na żądanie administratora przez serwer do centralnego zarządzania o:  wykrytym oprogramowaniu szkodliwym, wraz ze wskazaniem nazw stacji roboczych, gdzie oprogramowanie zostało wykryte,  wersjach baz sygnatur i wersjach oprogramowania antywirusowego, ze wskazaniem nazw stacji roboczych, na których występują określone wersje oprogramowania,  zainstalowanym innym oprogramowaniu,  wykaz zadań realizowanych przez agenty oprogramowania zainstalowane na stacjach roboczych, w określonym czasie,  zadaniach realizowanych przez system centralnego zarządzania w określonym czasie,  wynikach skanowania realizowanych w określonym czasie,  plikach przesłanych do chmury, w celu ich dokładnej analizy, w określonym czasie,  stacjach roboczych, na których oprogramowanie wykryło zagrożenie w określonym czasie,  obiektach poddanych kwarantannie,  zdarzeniach zarejestrowanych w dzienniku audytu.  Serwer/konsola centralnego zarządzania musi zapewniać obsługę powiadomień email, generować komunikaty SNMP oraz syslog wraz ze wsparciem dla przesyłania logów do oprogramowania SIEM. System musi zapewniać możliwość agregacji identycznych powiadomień występujących w określonej przez administratora jednostce czasu.  Serwer/konsola centralnego zarządzania musi zapewniać obsługę licencji na dostarczone oprogramowanie równoważne, umożliwiać dodawanie, synchronizacje licencji, wskazywać aktualne wykorzystanie oraz czas wygaśnięcia, wersje produktu na jaki jest udzielana licencja.  Serwer/konsola centralnego zarządzania musi zapewniać obsługę zadań zlecanych do wykonania na komputerach minimum w zakresie aktualizacji kluczy licencyjnych, instalacji pakietu oprogramowania antywirusowego, usunięcia zainstalowanego oprogramowania antywirusowego, instalacji oraz deinstalacji innego oprogramowania, wykonywania skryptów minimum vbs i powershell.  Serwer/konsola centralnego zarządzania musi zapewniać dostęp do logów diagnostycznych z modułów zabezpieczających, możliwość wygenerowania dziennika diagnostycznego dla komputera podlegającego ochronie.  Serwer/konsola centralnego zarządzania musi zapewniać dziennik zmian wprowadzanych przez administratorów dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.  Dodatkowe wymagania ogólne dla oprogramowania równoważnego:  Wszelkie komponenty rozwiązania równoważnego instalowane na komputerach i serwerach pracujących pod kontrolą systemu operacyjnego z rodziny Windows musza być dystrybuowane również w formie pakietów instalacyjnych msi, w celu ich łatwej, zdalnej instalacji na chronionych urządzeniach.  W przypadku oprogramowania równoważnego, należy zapewnić szkolenie z zakresu instalacji, wdrożenia i obsługi w zakresie zarządzania oprogramowaniem dla minimum 5 informatyków oraz należy zapewnić pomoc w sprawnym wdrożeniu oprogramowania przed dniem 01.01.2025. W tym celu należy zapewnić odpowiednio dłuższy okres aktualizacji oprogramowania równoważnego tak, aby było możliwe płynne zastąpienie aktualnie eksploatowanego oprogramowania, oprogramowaniem równoważnym, w terminie do 01.01.2025r. bez przesunięcia daty końca ważności o której mowa w Lp. 4 oraz należy zapewnić wsparcie w języku polskim przez cały okresaktualizacji. | |
| 2. | **Obsługiwane systemy operacyjne i oprogramowanie serwerowe:**  Dla stacji roboczych co najmniej Windows 10/11 w wersji 32 i 64 bitowej.  Dla serwerów plików co najmniej Windows 2012 R2, 2016, 2019, 2022, Linux RedHat 8 i pochodne. | |
| 3. | **Certyfikaty i pozostałe wymagania:**   * + - 1. Producent równoważnego oprogramowania antywirusowego musi być wymieniony na aktualnym raporcie „Magic Quadrant for Endpoint Protection Platforms” firmy Gartner.       2. Producent równoważnego oprogramowania antywirusowego musi być wymieniony na aktualnym raporcie Endpoint Prevention & Response (EPR) organizacji AV-Comparatives w sekcji strategic leaders. | |
| 4. | **Okres aktualizacji oprogramowania:** minimum jeden rok, koniec okresu aktualizacji oferowanego oprogramowania nie może być wcześniejszy, jak 31.12.2025 r. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 2. Oprogramowanie do przeprowadzania audytu stacji roboczych i kontroli działań użytkowników na stacjach roboczych** | | **Ilość – 1 komplet** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** przedłużenie wsparcia technicznego i prawa do aktualizacji oprogramowania Statlook na okres 1 roku (asysta serwisowa) dla 360 agentów i 6 konsol zarządzania wraz ze zwiększeniem liczby konsol do 7 łącznie.  Lub rozwiązanie równoważne o funkcjonalności umożliwiającej w szczególności:   1. Przeprowadzanie inwentaryzacji i audytu oprogramowania, zainstalowanego i przechowywanego na komputerach pracowników. Rozwiązanie równoważne musi zawierać komplet wzorców oprogramowania dostarczanych przez producenta rozwiązania, obejmujący minimum popularne oprogramowanie dostępne na platformę Windows wraz z możliwością tworzenia własnych wzorców. 2. Przeprowadzenie inwentaryzacji i audytu plików multimedialnych, przechowywanych na komputerach pracowników. Rozwiązanie równoważne musi zawierać komplet wzorców dla typów plików multimedialnych dostarczanych przez producenta oprogramowania, obejmujący popularne formaty multimedialne wraz z możliwością tworzenia własnych wzorców. 3. Przeprowadzanie inwentaryzacji i audytu sprzętu, monitoring zmian w konfiguracji komputerów w zakresie zmian w sprzęcie, jak i w oprogramowaniu. W ramach modułu inwentaryzacji rozwiązanie równoważne musi automatycznie pobierać dane dot. sprzętu z komputerów na których został zainstalowany agent oprogramowania a także umożliwiać ręczne dodawanie pozycji do wykazu zinwentaryzowanego sprzętu. Sprzęt musi być możliwy do opisania za pomocą osobnych atrybutów/pól: Typ (komputer, drukarka i wiele innych rodzajów sprzętu), numer inwentarzowy, numer seryjny, osoba odpowiedzialna, główny użytkownik, firma, dział, lokalizacja, wpływ (klasyfikacja rodo), kod kreskowy, opis, tagi, informacje odczytywane i uzupełniane automatycznie przez agenta: numer seryjny, główny użytkownik, nazwa DNS, adres IP, MAC adres, domena/grupa robocza, service tag, procesor, liczba rdzeni, pojemność pamięci RAM, pojemność dysku, karta graficzna, rozdzielczość ekranu. Pozostałe zasoby sprzętowe inwentaryzowane automatycznie przez agenta widoczne na szczegółowych raportach dot. sprzętu. Ponadto dane finansowe, informacja o gwarancji i jej terminie, informacje o umowie serwisowej. Z poziomu sprzętu musi być możliwe wskazanie (przypisanie) licencji wykorzystywanych przez dany sprzęt, użytkowników wykorzystujących dany sprzęt wraz z historią użycia sprzętu zbieraną przez agenta i historią zmian wprowadzanych manualnie, definicji własnych dodatkowych atrybutów oraz atrybutów automatycznie wprowadzanych przez agenta, zgłoszeniach w help desk wygenerowanych w kontekście danego sprzętu, załączników (skan np. faktur), notatek, historii zmian. Dodatkowo musi istnieć możliwość tworzenia zestawów/kompletów składających się z kilku urządzeń, wówczas wchodząc na poszczególne urządzenia musi być widoczne powiązanie pomiędzy nimi pozostałe urządzenia. 4. Zdalne wykonywanie zdefiniowanych przez administratora skryptów na monitorowanych komputerach w celu automatyzacji zadań administracyjnych. W tym obsługa skryptów cmd, powershell w raz z przechwytywaniem informacji zwrotnych generowanych przez skrypty, przechowywaniem historii wywołań skryptów z kontekście danego komputera wraz z uzyskaną informacją zwrotną. Dodatkowo przy wywołaniu skryptów musi być możliwość wskazania kontekstu bezpieczeństwa w jakim skrypt ma być uruchomiony minimum w zakresie: aktualnie zalogowany użytkownik, usługa lokalna, usługa sieciowa, system. 5. Automatyzacja procesów za pomocą predefiniowanych reguł - administrator definiuje akcje, które będą wykonywane przez rozwiązanie równoważne np. powiadomienie administratora. 6. Centralne zbieranie zalogowanych zdarzeń na komputerach podłączonych do oprogramowania wraz z możliwością filtrowania zdarzeń, które mają się znaleźć w centralnym repozytorium oraz wyszukiwanie na konsoli określonych wg. filtru zdarzeń. 7. Centralne monitorowanie stanu aktualizacji podłączonych stacji roboczych minimum z wykorzystaniem informacji zwracanych przez system Windows wraz z przechowywaniem historii zmian. 8. Monitoring pracy pracowników w zakresie czasu wykorzystania poszczególnych aplikacji, ze szczególnym uwzględnieniem czasu przeglądania Internetu oraz wskazaniem odwiedzanych stron przez pracowników (statystyka musi być pobierana minimum z przeglądarek: Edge, Firefox, Chrome, Opera) wraz z przechowywaniem danych historycznych. 9. Monitoring i raportowanie wydruków wraz z informacją o tytułach wydruków i liczbie wydrukowanych stron i typu wydruku (kolor/cz.b.) wraz z przechowywaniem danych historycznych. 10. Monitoring i raportowanie użycia nośników wymiennych wraz z informacją, jakie pliki zostały otworzone/zapisane wraz z przechowywaniem danych historycznych. 11. Możliwość blokowania nośników wymiennych, możliwość blokowania nośników wymiennych w tryb tylko do odczytu, do zapisu i do odczytu, blokada uruchamiania programów z nośnika wraz z przechowywaniem danych historycznych. Zezwolenie na użycie nośników wymiennych powinno być możliwe do zdefiniowana w kontekście danej osoby i danego nośnika, w kontekście nośnika (możliwy do użycia przez wszystkich) oraz osoby – możliwość użycia dowolnych nośników przez daną osobę. 12. Możliwość blokowania uruchamiania programów przez użytkowników i blokowania wybranych stron w sieci Internet. 13. Moduł help-desk’u, umożliwiający zgłaszanie przez pracowników problemów i obsługę zgłaszanych problemów przez pracowników obsługi technicznej (operatorów systemu). Pracownik tworząc zgłoszenie w systemie Windows objętym działaniem rozwiązania równoważnego musi mieć możliwość otwarcia formularza zgłoszeniowego bezpośrednio z zasobnika systemowego swojego komputera bez konieczności dodatkowego logowania się do systemu help-desk, a zmiany statusu zgłoszeń muszą być również widoczne w czasie zbliżonym do rzeczywistego jako powiadomienia z zasobnika systemowego. Ponadto klikając w zasobniku systemowym użytkownik musi mieć możliwość przejrzenia kilku swoich ostatnich zgłoszeń, ich otarcia w celu zapoznania się ze szczegółami rozwiązania bez konieczności dodatkowego logowania. 14. Moduł karty pracownika, umożliwiający pracownikowi w systemie Windows objętym działaniem oprogramowania z poziomu zasobnika systemowego otwarcie karty pracownika bez konieczności dodatkowego logowania i minimum zapoznanie się z przydzielonymi zasobami (sprzęt i licencje na oprogramowanie) statystyką swojej pracy (czas rozpoczęcia i zakończenia, czas pracy, czas przerw w poszczególnych dniach, czas pracy na poszczególnych programach – top 4 z możliwością zapoznania się ze szczegółami dot. czasu pracy w poszczególnych aplikacjach, informacjach o sporządzanych wydrukach w danym czasie i podłączonych nośnikach zewnętrznych po wskazaniu okresu czasowego). 15. Moduł raportowania, obejmujący wszelkie aspekty związane z audytami oprogramowania, bieżącą konfiguracją monitorowanych komputerów (sprzętową i programową) oraz prowadzeniem ewidencji posiadanego majątku w zakresie sprzętu i oprogramowania. Raporty muszą być możliwe do zapisania minimum w formacie pdf, xlsx, csv, txt, html, rtf. Ponadto przy przygotowywaniu raportów musi być możliwe dodawanie lub usuwanie kolumn, filtrowanie wyników itp. 16. Moduł umożliwiający rejestrowanie posiadanych licencji na oprogramowanie i korelowanie ich ręczne oraz automatyczne z wynikami przeprowadzonych audytów. Podczas rejestracji licencji musi być możliwe wskazane wcześniej zdefiniowanej reguły wykrywania oprogramowania oraz klucza produktu, tak aby system automatycznie korelował komputery na których jest zainstalowane dane oprogramowanie i umożliwiał półautomatyczne przypisywanie komputerów do licencji. W przypadku oprogramowania Microsoft system musi oprócz korelacji przy pomocy wzorca rozróżniać klucze produktów i przypisywać komputery na których jest zainstalowane oprogramowanie używające dany klucz produktu do danej licencji gdzie taki klucz jest wprowadzony. Ponadto podczas rejestracji licencji musi istnieć możliwość wskazania nazwy, wydawcy, typu licencji, języka, osoby odpowiedzialnej, głównego użytkownika, typu licencji (na urządzenie/na użytkownika/licencja sieciowa itp.), liczby posiadanych licencji, daty wygaśnięcia, daty zakończenia wsparcia, informacji finansowych, takich jak numer faktury, sprzedawca, cena, data nabycia, informacji o downgrade i upgrade, załączniki (skany faktur), notatki, historia zmian. 17. Funkcjonalność audytu oprogramowania musi wspierać administratora w ocenie stanu legalności zainstalowanego oprogramowania, poprzez rozróżnienie programów komercyjnych od programów, które mogą być użytkowane bez opłat oraz w sposób zautomatyzowany porównywać zarejestrowane w programie licencje na oprogramowanie z wynikami skanów oprogramowania zainstalowanego na komputerach. Moduł audytu oprogramowania musi uwzględniać części składowe, wchodzące w skład danego pakietu oprogramowania i raportować je w postaci jednego wpisu. 18. Moduł pomocy zdalnej, gdzie informatyk (operator systemu), ze swojej konsoli, może się podłączyć do pulpitu pracownika zgłaszającego problem w tym do sesji zdalnej podłączonej do danego komputera i dokonywać zdalnej diagnozy wraz z możliwością pobierania informacji o działających procesach w systemie zdalnym, edycji rejestru systemu zdalnego, pobierania i zapisywania plików na zdalny komputer. Pomoc zdalna musi umożliwiać: podgląd działań pracownika bez przejmowania jego klawiatury i myszy, interakcje z pracownikiem wraz z możliwością blokady klawiatury i myszy pracownika. Uruchomienie pomocy zdalnej musi generować po stronie pracownika komunikat informujący o tym fakcie oraz na ekranie pracownika musi stale się wyświetlać stosowna informacja niemożliwa do usunięcia przez pracownika. Moduł pomocy zdalnej nie może wymuszać wylogowania pracownika z jego sesji. Pomoc zdalna musi być realizowana za pomocą komunikacji szyfrowanej i musi być przeprowadzana przez system stosowna autoryzacja wewnętrzna, nie dopuszcza się rozwiązań opartych o standardowy VNC. Rozwiązanie musi również przechowywać historie sesji zdalnych w postaci informacji takich jak nazwa komputera i nazwę operatora realizującego pomoc zdalną, komputer i nazwa pracownika do którego połączenie zostało nawiązanie, czas rozpoczęcia, czas trwania, informacje o typie sesji, informacje czy wyświetlony został komunikat informujący pracownika o rozpoczęciu pomocy zdalnej, informacje o tym czy połączenie było realizowane z dostępem do klawiatury i myszy pracownika, liczbie kliknięć myszką i wprowadzonych znaków z klawiatury przez operatora, informacje o blokadzie klawiatury i myszy pracownika. 19. Funkcja wyświetlania okresowo aktualizowanego widoków ekranów komputerów pracowników na konsoli operatora systemu. 20. Moduł wspomagający zarządzanie zgodnością organizacji z wymaganiami określonymi w RODO, umożliwiający w szczególności prowadzenie rejestru czynności przetwarzania, zbiorów, pracowników, przypisywanie zbiorów do czynności, rejestrowanie dostępów do zbiorów, naruszeń bezpieczeństwa przetwarzania informacji, prośby o usunięcie danych ze zbioru, rejestr czynności przetwarzania, rejestr szkoleń związanych z przetwarzaniem danych osobowych, rejestr upoważnień do przetwarzania danych. 21. Moduł wspierający realizacje zadań związanych z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/1937 dotyczącą tzw. sygnalistów, umożliwiający obsługę anonimowych zgłoszeń. 22. Konsola zarządzania musi umożliwiać nadawanie poszczególnym operatorom systemu różnych poziomów uprawnień minimum w zakresie: pełne uprawnienia do wszystkich modułów, ograniczone uprawnienia dla kierownika danego zespołu gdzie dany kierownik ma dostęp tylko do wybranych funkcji (między innymi w zakresie raportowanie informacji o pracy pracowników, pomoc zdalna pracownikom, okresowo aktualizowany widok ekranów komputerów pracowników) oraz tylko do wybranych komputerów i pracowników przypisanych do danego działu. Ponadto konsola musi umożliwiać przypisywanie uprawnień w zakresie funkcji realizowanych w ramach RODO (ADO, IOD, ASI) i funkcji realizowanych w ramach obsługi sygnalistów. 23. Komunikacja pomiędzy agentem a serwerem musi być odpowiednio zabezpieczona przed podsłuchem i przejęciem przez obcy serwer. 24. Rozwiązanie równoważne musi wykorzystywać do działania nielimitowane bazy danych dostępne bezpłatnie, takie jak PostgreSQL. 25. Rozwiązanie równoważne musi umożliwiać obsługę minimum 360 stacji roboczych i co najmniej 7 konsol zarządzania. Przy czym licencjonowanie dla konsol musi umożliwiać posiadanie przez Zamawiającego większej liczby uprawnionych operatorów, gdzie system umożliwia dostęp maksymalnie 7 równoczesnym sesjom i limituje ten dostęp w ramach dostępnego limitu równoczesnych sesji. 26. W przypadku rozwiązania równoważnego, należy zapewnić szkolenie z zakresu instalacji, wdrożenia i obsługi rozwiązania dla minimum 5 informatyków oraz należy zapewnić pomoc w sprawnym wdrożeniu rozwiązania. 27. Rozwiązanie równoważne musi być licencjonowane w formie licencji bezterminowej. 28. Rozwiązanie równoważne należy dostarczyć ze wsparciem technicznym i prawem do aktualizacji ważnym minimum przez okres 1 rok od dnia dostawy. 29. W przypadku oprogramowania równoważnego należy je dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024. | |
| 2. | **Obsługiwane systemy operacyjne:** minimum Windows 10/11 w wersji 32 i 64 bitowej oraz Windows 2012 R2, 2016, 2019, 2022. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 3. Oprogramowanie serwerowe – obsługujące wirtualizację** | | **Ilość – 1 komplet** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** subskrypcja roczna oprogramowania vSphere Standard zapewniająca możliwość eksploatacji tego oprogramowania na serwerach wyposażonych łącznie w 168 rdzeni procesorów i oprogramowania vCenter do zarządzania oprogramowaniem vSphere Standard (5 serwerów z tego 2 serwery gdzie każdy jest wyposażony w 2 procesory po 18 rdzeni i pozostałe serwery wyposażone w 2 procesory po maksimum 16 rdzeni każdy). Subskrypcje należy dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024.  Lub oprogramowanie równoważne, dające prawo do jego instalacji na minimum 5 serwerach fizycznych o architekturze x86-64, obsługujące co najmniej 2 wielordzeniowe procesory fizyczne na każdym serwerze zawierające ilość rdzeni opisaną powyżej na każdy procesor i obsługą minimum 1TB pamięci RAM zainstalowanej w każdym z serwerów, umożliwiające przypisanie co najmniej 32 procesorów, 128GB pamięci RAM i 10 kart sieciowych do każdej maszyny wirtualnej wykreowanej w tym oprogramowaniu, z możliwością obsługi co najmniej 60 maszyn wirtualnych na każdym serwerze, w miarę dostępnych zasobów serwera fizycznego, obsługujące dyski lokalne serwera i dyski zdalne przez protokół NFS, iSCSI, FC (sieć SAN), obsługujące karty sieciowe 1 i 10Gb Ethernet zainstalowane w serwerze, umożliwiające bezpośrednie podłączenie urządzenia fizycznego serwera (karty SAS, napęd taśmowy podłączony do karty SAS w serwerze fizycznym, port szeregowy serwera fizycznego, port USB serwera fizycznego) do wykreowanej maszyny wirtualnej, tak aby ta maszyna sterowała urządzeniem w sposób wyłączny i bezpośrednio, za pośrednictwem właściwych sterowników dla ww. urządzenia. Z prawem do aktualizacji tego oprogramowania w okresie minimum 1 roku od daty udzielenia licencji Zamawiającemu do najnowszych wersji oprogramowania, gdy taka wersja zostanie opublikowana oraz prawem do wsparcia, w okresie 1 roku, od daty udzielenia licencji Zamawiającemu, licencjonowane w formie licencji bezterminowej lub subskrypcji rocznej. Oprogramowanie równoważne musi zapewniać podobną wydajność pracy wykreowanych na nim maszyn wirtualnych zarówno w zakresie IOPS systemu dyskowego, wydajności procesora, jak i przepustowości pamięci RAM. Oprogramowanie równoważne musi posiadać system centralnego zarządzania poszczególnymi instancjami zainstalowanymi na serwerach fizycznych w ramach licencji, wspierający między innymi automatyzujące działania takie, jak migracja maszyny wirtualnej na działający serwer w przypadku awarii serwera, na którym dana maszyna pracowała. Oprogramowanie równoważne musi zapewniać możliwość migracji maszyn wirtualnych pomiędzy serwerami fizycznymi w trakcie ich pracy oraz offline. Oprogramowanie równoważne musi zapewniać wsparcie dla maszyn wirtualnych wykorzystujących co najmniej następujące systemy operacyjne: Windows, Linux, UnixWare 7.1.4.  W przypadku dostarczenia oprogramowania równoważnego, należy zapewnić odpowiednie szkolenia dla administratorów z zakresu obsługi i eksploatacji tego oprogramowania oraz migrację środowiska wirtualnego, opartego na oprogramowaniu VMware Essentials Plus Kit, na nowe oprogramowanie.  W przypadku oprogramowania równoważnego należy dostarczyć odpowiednie oprogramowanie do wykonywania kopii zapasowych, o którym jest mowa w poz. 4.  W przypadku oprogramowania równoważnego należy je dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 4. Oprogramowanie do wykonywania kopii zapasowych** | | **Ilość – 1 komplet** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** przedłużenie co najmniej podstawowego wsparcia technicznego i prawa do aktualizacji na okres 1 roku dla oprogramowania Veeam Backup and Replication Standard licencjonowane dla 14 procesorów dla VMware vSphere (numer aktualnie posiadanego kontraktu: 03204770) oraz przedłużenie wsparcia technicznego i prawa do aktualizacji dla 10 instancji Veeam Data Platform Foundation w wersji perpetual na okres 1 roku.  Lub oprogramowanie równoważne zapewniające możliwość wykonywania kopii zapasowych maszyn wirtualnych pracujących na serwerach VMware vSphere lub na oprogramowaniu, o którym mowa w poz. 3, w przypadku dostarczania produktu równoważnego, o którym tam mowa, zapewniające co najmniej następujące możliwości: wykonywanie kopii zapasowych maszyn wirtualnych bez konieczności instalowania na tych maszynach agenta, wykonywanie kopii zapasowych aplikacji zainstalowanych na maszynach wirtualnych Windows AD, MS SQL, Exchange w sposób w pełni konsystentny, z możliwością zarządzania logami transakcyjnymi tych aplikacji, z możliwością wykonywania skryptów przed rozpoczęciem wykonywania kopii i po zakończeniu wykonywania kopii umożliwiające integracje kopii zapasowych z innymi aplikacjami, wykonywanie kopii zapasowych w trybie całościowym i przyrostowym, możliwość tworzenia kopii całościowej w sposób syntetyczny na podstawie kopii przyrostowych, wykorzystywanie mechanizmu kompresji i deduplikacji do zmniejszenia ilości przechowywanych danych, obsługa trybu CBT, wykorzystanie migawek oprogramowania witalizacyjnego i dalsze wykonywania kopii zapasowych bazujące na wcześniej wykonanej migawce, wykonywanie kopii maszyn wirtualnych w trakcie ich pracy bez wpływu na ich pracę, jak i maszyn wyłączonych, replikacja maszyn wirtualnych na inny serwer fizyczny, wyposażony w oprogramowanie do wirtualizacji, zgodnie z harmonogramem oraz w czasie zbliżonym do rzeczywistego bez wykorzystywania standardowych migawek, możliwość praktycznie natychmiastowego odtworzenia maszyny wirtualnej z kopii zapasowej przy wykorzystaniu wystawianego przez oprogramowanie równoważne udziału sieciowego NFS, bazującego na kopii maszyny po przez uruchomienie maszyny wirtualnej bezpośrednio z kopii i rozpoczęcie jej odzyskiwania na zasoby główne serwera w trakcie pracy maszyny, obsługa co najmniej 2 napędów taśmowych LTO do wykonywania archiwizacji maszyn i plików na taśmę wraz z możliwością podłączenia tych napędów zarówno lokalnie, jak i zdalnie, za pośrednictwem odpowiedniego modułu oprogramowania dołączonego do oprogramowania równoważnego, w celu minimalizacji pasma sieciowego w lokalizacjach zdalnych, obsługa harmonogramów umożliwiających wykonywanie kopii zapasowych i replikacji danych w określonych odstępach czasowych, obsługa wykonywania kopii przechowywanej w co najmniej 2 magazynach jednocześnie, z możliwością osobnego określenia retencji przechowywanych kopii oraz harmonogramu replikacji kopii do drugiego magazynu, obsługa magazynów chmurowych do przechowywania kopii zapasowych, obsługa odtwarzania maszyn wirtualnych na dotychczasowym serwerze, jak i nowym serwerze wirtualizacji, obsługa odtwarzania pojedynczych plików maszyn wirtualnych opartych na systemach operacyjnych co najmniej Windows i Linux, obsługa co najmniej 4 zdalnych magazynów przechowywania danych tak, aby zminimalizować pasmo sieciowe przy wykonywaniu kopii w lokalizacjach zdalnych. Podczas tworzenia kopii w lokalizacji zdalnej do magazynu umieszonego w tej lokalizacji transfer danych musi nie wychodzić poza tą lokalizację. Oprogramowanie równoważne musi umożliwiać równoczesną obsługę serwerów fizycznych pojedynczych i serwerów zarządzanych przez oprogramowanie do centralnego zarządzania. Oprogramowanie równoważne musi zapewniać obsługę lokalnych magazynów danych tworzonych w oparciu o system Windows oraz Linux, ponadto musi wspierać magazyny typu SMB, NAS i magazyny typu Immutability budowane w oparciu o system Linux i możliwości systemu plików XFS. Wydajność lokalnych magazynów opartych o system Linux musi być porównywalna z wydajnością lokalnych magazynów budowanych w oparciu o system Windows na tych samych zasobach sprzętowych. Oprogramowanie równoważne musi obsługiwać integracje z macierzami dyskowymi minimum dla macierzy IBM Storwize. Oprogramowanie równoważne musi posiadać prawo do aktualizacji i podstawowego wsparcia technicznego w okresie jednego roku od daty udzielenia licencji Zamawiającemu. Licencja na oprogramowanie równoważne musi być bezterminowa. Oprogramowanie równoważne musi zapewniać możliwość obsługi co najmniej 7 serwerów fizycznych wyposażonych w 2 procesory każdy lub oprogramowanie równoważne musi zapewniać możliwość wykonywania kopii zapasowych dla minimum 60 maszyn wirtualnych lub pojemność chronionych zasobów serwerowych minimum 40TB (pojemność przechowywanych kopi zapasowych odpowiednio inna, zależna od przyjętej polityki przechowywania kopii zapasowych, poziomu kompresji i sprawności mechanizmu deduplikacji) oraz minimum 2 TB danych przechowywanych na taśmach LTO w ramach przechowywania na taśmach LTO kopii zasobów plikowych nie licząc pojemności wykorzystywanej przez przechowywane na taśmach kopie maszyn wirtualnych (łącznie 80TB przechowywanych na taśmach LTO). Licencja oprogramowania równoważnego musi zapewniać możliwość dalszego zwiększenia liczby obsługiwanych serwerów fizycznych lub maszyn wirtualnych poprzez zakup i dodanie przez Zamawiającego kolejnych licencji. Licencja na oprogramowanie równoważne musi zawierać w sobie licencje na oprogramowanie bazy danych wykorzystywanej przez oprogramowanie równoważne lub oprogramowanie równoważne musi wykorzystywać do tego celu oprogramowanie bazy danych Postgresql.  W przypadku dostarczenia oprogramowania równoważnego, należy zapewnić odpowiednie szkolenia dla administratorów z zakresu obsługi i eksploatacji tego oprogramowania oraz migrację środowiska kopii zapasowych na nowe oprogramowanie.  W przypadku oprogramowania równoważnego należy je dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 5. Pakiet oprogramowania do edycji grafiki - Typ I** | | **Ilość – 1 licencja** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** pakiet wsparcia na jeden rok (CorelDRAW Graphics Suite Enterprise CorelSure Maintenance (1 Yr)) do oprogramowania CorelDraw w wersji Graphic Suite posiadanego przez Zamawiającego. Pakiet należy dostarczyć w terminie do 30 listopada 2024 r. tak aby przedłużyć posiadany przez Zamawiającego pakiet.  Lub oprogramowanie równoważne spełniające poniższe wymagania:  Oprogramowanie umożliwiające edycję grafiki wektorowej oraz map bitowych, składu stron, edycji zdjęć, trasowania, przygotowywania grafik internetowych i animacji.  Oprogramowanie w polskiej wersji językowej.  Oprogramowanie działające co najmniej na systemie operacyjnym Windows w wersjach 10 i 11, zarówno 32 jak i 64 bitowych.  100% zgodność z formatem CDR w wersjach CorelDraw w wersji Graphic Suite 24.3 i niższej (zarówno odczyt jak i edycja) bez konieczności dodatkowej konwersji.  Dostępne materiały szkoleniowe w formie wideo.  Dołączona biblioteka zdjęć, cyfrowych obrazów, grafik wektorowych, czcionek oraz szablonów, ramek i wzorów.  Oprogramowanie równoważne musi posiadać prawo do aktualizacji w okresie jednego roku od daty udzielenia licencji Zamawiającemu.  Oprogramowanie musi być licencjonowane w formie licencji bezterminowej.  Użytkownicy są przeszkoleni z zakresu obsługi programu Corel Draw. Dostawca zobowiązany jest przeszkolić dwóch użytkowników w przypadku zaproponowania oprogramowania równoważnego.  W przypadku oprogramowania równoważnego należy je dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024. | |
| 2. | **Licencja:** bezterminowa,pudełkowa lub elektroniczna, korporacyjna lub rządowa | |
| 3. | **Platforma systemowa:** Windows 10/11 | |

|  |  |  |
| --- | --- | --- |
| **Poz. 6. Pakiet oprogramowania do edycji grafiki - Typ II** | | **Ilość – 1 licencja** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | Wymagania ogólne: możliwość edycji, tworzenia grafiki wektorowej oraz map bitowych, składu stron, edycji zdjęć, trasowania, przygotowywania grafik internetowych i animacji, możliwość otwierania i edycji plików przygotowanych co najmniej za pomocą oprogramowania CorelDraw w wersji Graphic Suite 2024 i niższej bez konieczności dodatkowej konwersji, oprogramowanie w polskiej wersji językowej jeśli taka wersja istnieje, w przeciwnym przypadku w angielskiej wersji językowej.  Lub oprogramowanie równoważne spełniające poniższe wymagania:  1. Oprogramowanie umożliwiające edycję grafiki wektorowej oraz map bitowych, składu stron, edycji zdjęć, trasowania, przygotowywania grafik internetowych i animacji.  2. Oprogramowanie w polskiej wersji językowej.  3. Oprogramowanie działające co najmniej na systemie operacyjnym Windows w wersjach 10 i 11, zarówno 32 jak i 64 bitowych.  4. 100% zgodność z formatem CDR w wersjach CorelDraw w wersji Graphic Suite 2024 i niższej (zarówno odczyt jak i edycja) bez konieczności dodatkowej konwersji.  5. Dostępne materiały szkoleniowe w formie wideo.  6. Dołączona biblioteka zdjęć, cyfrowych obrazów, grafik wektorowych, czcionek oraz szablonów, ramek i wzorów.  7. Użytkownicy są przeszkoleni z zakresu obsługi programu Corel Draw. Dostawca zobowiązany jest przeszkolić dwóch użytkowników w przypadku zaproponowania oprogramowania równoważnego. | |
| 2. | **Licencja:** bezterminowa,pudełkowa lub elektroniczna, korporacyjna lub rządowa | |
| 3. | Roczne wsparcie w postaci prawa do aktualizacji oprogramowania o ile producent wyda jego nową wersję. | |
| 4. | **Platforma systemowa:** Windows 10/11 | |

|  |  |  |
| --- | --- | --- |
| **Poz. 7. Pakiet oprogramowania do edycji grafiki - Typ III** | | **Ilość – 1 subskrypcja** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** przedłużenierocznej subskrypcji oprogramowania Adobe Photoshop CC for Teams w polskiej wersji językowej przeznaczonej dla systemu Windows (numer aktualnej umowy VIP - 0E372DCF8C5CB926E8DA). Subskrypcje należy dostarczyć w terminie do 09 grudnia 2024 r.  Lub oprogramowanie równoważne spełniające poniższe wymagania:  Zakres funkcjonalny oprogramowania równoważnego możliwie zbieżny z zakresem funkcjonalnym oprogramowania wzorcowego wskazanego przez Zamawiającego. Formaty danych wejściowych i wyjściowych muszą być zbieżne i odpowiadać przynajmniej liczbie i typowi formatów dla programu wzorcowego wskazanego przez Zamawiającego. Warunki licencji oprogramowania nie mniej korzystne niż warunki programu wskazanego. Wymagania muszą zostać spełnione poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.  Ponadto oprogramowanie równoważne musi zapewniać możliwość:  Eksportowania zasobów,  Stosowania wielu instancji stylów warstw,  Korzystania z pędzla korygującego w czasie rzeczywistym,  Przesuwania i rozszerzania z uwzględnieniem zawartości i funkcją skalowania i obracania,  Korzystania z automatycznej funkcji wypełniania z uwzględnieniem zawartości do połączonych obrazów panoramicznych,  Tworzenia zestawów linii pomocniczych i ustawień predefiniowanych,  Korzystania z połączonych obiektów inteligentnych,  Korzystania z ulepszonych kompozycji warstw,  Korzystania z efektów ruchu i szumu addytywnego w galerii rozmyć,  Korzystania z maski ostrości,  Obsługi druku 3D,  Wyszukiwania i natychmiastowego podglądu czcionek,  Obsługi wysokich rozdzielczości w systemie Windows,  Korzystania z narzędzia pędzla korygującego, inteligentnego wyostrzenia oraz próbkowania w górę,  Korzystania z demonstracji materiałów,  Redukcji potrząśnięć aparatem fotograficznym,  Korzystania z intuicyjnej produkcji wideo,  Korzystania z narzędzia do kadrowania,  Korzystania z galerii rozmyć,  Migracji i udostępniania ustawień predefiniowanych,  Automatycznych korekcji,  Automatycznego odzyskiwania,  Zapisywania w tle,  Łatwego zaznaczania złożonych elementów,  Wypełniania z uwzględnianiem zawartości,  Korzystania z wypaczenia marionetkowego,  Obróbki obrazów HDR,  Korzystania z efektów malowania,  Automatycznej korekcji obiektywu,  Automatycznego mieszania obrazów,  Płynnego panoramowania i powiększania,  Płynnego obracania obszaru roboczego,  Skalowania z uwzględnieniem zawartości,  Korzystania z bezpiecznych inteligentnych filtrów,  Automatycznego wyrównywania i mieszania warstw,  Scalania do 32-bitowych obrazów HDR,  Konwersji na obrazy czarno-białe,  Dopasowania krzywych,  Klonowania i naprawiania z opcjami dostosowania,  Oprogramowanie musi być fabrycznie nowe, nigdy nie aktywowane na innym urządzeniu,  Oprogramowanie winno być dostarczone wraz ze stosownymi oryginalnymi atrybutami legalności, np. poprzez rejestrację na stronie zarządzania licencjami producenta oprogramowania.  Oprogramowanie działające co najmniej na systemie operacyjnym Windows w wersjach 10 i 11 64 bitowych,  100% zgodność z formatem PSD w wersjach Photoshop (zarówno odczyt jak i edycja) bez konieczności dodatkowej konwersji,  Licencjonowane w formie subskrypcji lub bezterminowo wraz z rocznym wsparciem i prawem do aktualizacji oprogramowania,  Użytkownicy są przeszkoleni z zakresu obsługi programu Photoshop. Dostawca zobowiązany jest przeszkolić dwóch użytkowników w przypadku zaproponowania oprogramowania równoważnego.  W przypadku oprogramowania równoważnego należy je dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024. | |
| 3. | **Platforma systemowa:** Windows 10/11 | |

|  |  |  |
| --- | --- | --- |
| **Poz. 8. Oprogramowanie do obsługi systemu monitoringu wizyjnego** | | **Ilość – 1 licencja** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** aktualizacja oprogramowania go1984 edycja Ultimate, dająca prawo do korzystania z nowych wersji oprogramowania, powstałych minimum w okresie jednego roku od daty rocznicy udzielenia licencji na aktualizację Zamawiającemu, wraz z bezpłatnym wsparciem na okres jednego roku od wcześniej wymienionej daty.  Lub oprogramowanie równoważne o podobnej funkcjonalności w zakresie nielimitowanej obsługi kamer IP, wideo serwerów IP w tym kamer i wideo serwerów, będących w posiadaniu Zamawiającego (Axis, Vivotek), metod składowania i prezentacji danych, obsługi wielu monitorów, obsługi strumieni video kodowanych kodekiem H.264 i H.265 (HEVC), możliwości płynnego przeglądania zarejestrowanych obrazów zarówno do przodu jak i do tyłu z możliwością przyspieszenia przeglądu minimum 8 razy, wykorzystania wsparcia sprzętowego przy przewarzaniu strumieni za pomocą karty graficznej (GPU AMD, NVIDIA, Intel), zapewnienie wsparcia technicznego i prawa do aktualizacji na okres jednego roku od daty udzielenia licencji Zamawiającemu, licencja bezterminowa.  W przypadku oprogramowania równoważnego należy je dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024. | |
| 2. | **Pozostałe:** Oprogramowanie w polskiej wersji językowej, jeśli taka wersja istnieje, w przeciwnym przypadku w angielskiej wersji językowej. | |
| 3. | **Platforma systemowa:** co najmniej Windows 10/11. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 9. Subskrypcja oprogramowania** | | **Ilość – 14 subskrypcji** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** przedłużenie na kolejny rok subskrypcji na oprogramowanie Microsoft 365 Business Standard dla 14 użytkowników. W ramach subskrypcji wymagana jest możliwość użytkowania oprogramowania z pakietu Office: Word, Excel, PowerPoint, Access, Outlook oraz możliwość korzystania z funkcji pracy zespołowej i komunikacji za pośrednictwem oprogramowania Teams z możliwością tworzenia spotkań online dla minimum 500 uczestników jednocześnie, planowania harmonogramów spotkań, zapewniająca dostęp gościa do usługi Teams. Oprogramowanie z pakietu Office musi być dostępne w chmurze producenta oraz do instalacji stacjonarnej na komputerach użytkowników subskrypcji. Subskrypcja musi zapewniać możliwość podpisania/przedłużenia umowy powierzenia danych osobowych pomiędzy Zamawiającym a podmiotem realizującym subskrypcję.  Lub rozwiązanie równoważne zapewniające możliwość edycji plików Microsoft Office – Word, Excel, PowerPoint, Outlook. Publuisher, Access. Uwaga nie dopuszcza się przypadku gdy pliki Microsoft Office po otwarciu w oprogramowaniu równoważnym będą wymagać ponownego formatowania, wygląd dokumentów będzie odbiegał od wyglądu dokumentów otwieranych w oprogramowaniu Microsoft Office, konieczna będzie konwersja dokumentów w tym przepisanie makr na nowy język. Ponadto wymagane jest aby oprogramowanie równoważne bezproblemowo współpracowało z oprogramowaniem SyriuszStd i  PSZ.eDok. Rozwiązanie równoważne musi zapewniać możliwość pracy zespołowej – tworzenia spotkań online dla minimum 500 uczestników jednocześnie, zapewniać możliwość planowania harmonogramów spotkań, zapewniać dostęp gościa i nie wymagać logowania dla zwykłych uczestników do usługi spotkań online, umożliwiać przy tworzeniu spotkania definiowanie między innymi: czy niezalogowane osoby mogą pomijać poczekalnie, czy mają zablokowaną kamerę i mikrofon, czy funkcja chatu jest dostępna, czy spotkanie jest nagrywane, czy dostępne są automatyczne napisy. Rozwiązanie równoważne musi zapewniać możliwość podpisania umowy powierzenia danych osobowych pomiędzy Zamawiającym a podmiotem zapewniającym rozwiązanie równoważne oraz musi być zapewnione prawo do aktualizacji na okres jednego roku od daty udzielenia licencji Zamawiającemu.  W przypadku oprogramowania równoważnego należy je dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 10. Oprogramowanie narzędziowe - Typ I** | | **Ilość – 10 licencji** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** przedłużenie rocznego wsparcia do oprogramowania Oracle Java 8 JRE wraz ze zmniejszeniem liczby komputerów na których można zainstalować wspieraną wersję oprogramowania z 70 do 10, dające prawo do instalacji na komputerach użytkowników najnowszej wersji oprogramowania opublikowanej przez producenta w stosunku do wersji dostępnej bezpłatnie Oracle Java 8 JRE Update 202 (Java SE Desktop Subscription).  Lub rozwiązanie równoważne zapewniające możliwość bezawaryjnego uruchamiania na komputerach pracowników posiadanego przez Zamawiającego oprogramowania wykorzystującego pliki z rozszerzeniem .jnlp wymagającego do pracy środowiska Oracle Java JRE 8 Update 202 i nowszych waz z rocznym wparciem technicznym i prawem do aktualizacji. W przypadku oprogramowania równoważnego należy je dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 11. Oprogramowanie narzędziowe – Typ II** | | **Ilość – 2 licencje** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** Oprogramowanie Visual Studio 2022 Professional lub nowsze  Lub oprogramowanie równoważne zapewniające możliwość tworzenia oprogramowania w językach programowania Visual Basic, C# na platformę Windows z wykorzystaniem bibliotek programistycznych .Net, języka , C++ z wykorzystaniem Windows 11 SDK, możliwość tworzenia oprogramowania Web w oparciu o ASP.NET, Python, Node.js, zapewniająca podpowiadanie składni, możliwość debugowania tworzonych aplikacji w oprogramowaniu równoważnym w trakcie pracy tworzonych aplikacji. Rozwiązanie równoważne musi zapewniać Zamawiającemu prawo do aktualizacji w ramach zaoferowanej wersji podobnie jak jest to realizowane w przypadku oprogramowania Visual Studio 2022 Professional. | |
| 2. | **Typ licencjonowania:** Grupowe bezterminowe lub pudełkowe bezterminowe. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 12. Oprogramowanie narzędziowe – Typ III** | | **Ilość – 1 komplet** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** Aktualizacja oprogramowania Reboot Restore Rx Pro posiadanego przez Zamawiającego (9 licencji, wersja 11.x) wraz ze zwiększeniem liczby licencji do 10 łącznie i zapewnieniem wsparcia i aktualizacji głównych wersji oprogramowania przez okres minimum trzech lat.  Lub oprogramowanie równoważne zapewniające:   1. Obsługę minimum 10 komputerów z systemem Windows 10/11. 2. Ochronę systemu Windows przed nieautoryzowanymi zmianami. 3. Ochronę stanu dysku twardego komputera z systemem Windows przed nieautoryzowanymi zmianami. 4. Przystosowane do pracy w publicznych punktach obsługi. 5. Zapewniające automatycznie przywracanie stanu przy ponownym uruchomieniu komputera, wylogowaniu użytkownika oraz co określony czas. 6. Umożliwiające zdefiniowanie okna serwisowego w czasie którego komputer będzie mógł pobrać aktualizację dla systemu Windows i oprogramowania antywirusowego. 7. Posiadające możliwość zarządzania oprogramowaniem przez sieć LAN. 8. Umożliwiające zdefiniowanie miejsca na dysku komputera które nie podlega funkcji przywracania - zapisane pliki nie są wymazywane w procesie przywracania. 9. Wykorzystujące algorytm AES256 do szyfrowania danych aby wymieniowa możliwość dokonania zmiany na komputerze. 10. Wsparcie i aktualizacje przez okres minimum trzech lat. | |
| 2. | **Typ licencjonowania:** bezterminowa | |
| 3. | **Platforma systemowa:** co najmniej Windows 10/11. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 13. Oprogramowanie narzędziowe – Typ IV** | | **Ilość – 1 subskrypcja** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** Roczna subskrypcja oprogramowania Acrobat Pro for Enterprise dla administracji. Subskrypcje należy dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024  Lub oprogramowanie równoważne zapewniające:   1. Możliwość definiowania przez Administratora funkcjonalności oprogramowania, które są dostępne dla użytkowników. 2. Możliwość pracy oprogramowania bez dostępu do sieci Internet i usług chmurowych producenta oprogramowania. 3. Zakres funkcjonalny oprogramowania równoważnego możliwie zbieżny z zakresem funkcjonalnym oprogramowania wzorcowego wskazanego przez Zamawiającego. Warunki licencji oprogramowania nie mniej korzystne niż warunki programu wskazanego. Wymagania muszą zostać spełnione poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. 4. Edytowanie tekstu i obrazów oraz zmienianie kolejności i usuwanie stron w plikach PDF 5. Konwertowanie plików PDF i eksportowanie ich zawartości do programów Word, Excel oraz PowerPoint. 6. Podpisywanie dokumentów, uzyskiwanie podpisów i śledzenie odpowiedzi w czasie rzeczywistym. 7. Portal internetowy do zmieniania przydziałów licencji. 8. Redagowanie w celu trwałego usunięcia poufnych i widocznych informacji z plików PDF. 9. Gromadzenie podpisów elektronicznych osób wypełniających formularz internetowy. 10. Dodawanie logo marki do umów i wysyłanie formularzy PDF do natychmiastowego przekształcenia w formularze internetowy. 11. W przypadku oprogramowania równoważnego należy je dostarczyć w terminie określonym w umowie liczonym od dnia 9 grudnia 2024. | |
| 2. | **Typ licencjonowania:** bezterminowa | |
| 3. | **Platforma systemowa:** co najmniej Windows 10/11. | |

|  |  |  |
| --- | --- | --- |
| **Poz. 14. Oprogramowanie biurowe** | | **Ilość – 60 licencji** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** oprogramowanie Microsoft Office 2024 Home & Business  Lub oprogramowanie równoważne o podobnej funkcjonalności, wyposażone w interfejs API zgodny z oprogramowaniem Office oraz zapewniające bezobsługowe (nie wymagające wykonania dodatkowych czynności takich jak konwersja czy przepisanie oprogramowania makr na nowy język) działanie makr i programów napisanych w języku VBA, zawartych w dokumentach użytkowanych przez Zamawiającego. Bezproblemowa współpraca z systemem SyriuszStd i PSZ.eDok. W przypadku PSZ.eDok oprogramowanie to udostępnia w pakiecie Office dodatkowe menu do obsługi systemu PSZ.eDok, wymagane jest aby taka funkcjonalność była dostępna również w przypadku oprogramowania równoważnego. Przy otwieraniu dokumentów sporządzonych w oprogramowaniu Office za pomocą oprogramowania równoważnego, dokumenty nie mogą zmieniać postaci wizualnej, wymagać poprawek formatowania itp.  Ponadto oprogramowanie równoważne musi być kompatybilne z serwerami Exchange posiadanymi przez Zamawiającego w zakresie obsługi poczty elektronicznej, kalendarzy, folderów publicznych i obiektów współdzielonych utworzonych w folderach publicznych, zadań, nadawaniem uprawnień do dostępu i współdzieleniem zasobów.  W przypadku dostarczenia oprogramowania równoważnego, należy zapewnić odpowiednie szkolenia dla liczby użytkowników odpowiadającej liczbie licencji z zakresu obsługi i eksploatacji tego oprogramowania. | |
| 2. | **Platforma systemowa:** co najmniej Windows 10/11 w wersji 32 i 64 bitowej. | |
| 3. | **Typ licencjonowania:** bezterminowe. | |

* + - 1. **Oprogramowanie komputerowe wchodzące w zakres zamówienia opcjonalnego:**

|  |  |  |
| --- | --- | --- |
| **Poz. 1. Oprogramowanie biurowe** | | **Ilość – 40 licencji** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** | |
| 1. | **Wymagania ogólne:** oprogramowanie Microsoft Office 2024 Home & Business  Lub oprogramowanie równoważne o podobnej funkcjonalności, wyposażone w interfejs API zgodny z oprogramowaniem Office oraz zapewniające bezobsługowe (nie wymagające wykonania dodatkowych czynności takich jak konwersja czy przepisanie oprogramowania makr na nowy język) działanie makr i programów napisanych w języku VBA, zawartych w dokumentach użytkowanych przez Zamawiającego. Bezproblemowa współpraca z systemem SyriuszStd i PSZ.eDok. W przypadku PSZ.eDok oprogramowanie to udostępnia w pakiecie Office dodatkowe menu do obsługi systemu PSZ.eDok, wymagane jest aby taka funkcjonalność była dostępna również w przypadku oprogramowania równoważnego. Przy otwieraniu dokumentów sporządzonych w oprogramowaniu Office za pomocą oprogramowania równoważnego, dokumenty nie mogą zmieniać postaci wizualnej, wymagać poprawek formatowania itp.  Ponadto oprogramowanie równoważne musi być kompatybilne z serwerami Exchange posiadanymi przez Zamawiającego w zakresie obsługi poczty elektronicznej, kalendarzy, folderów publicznych i obiektów współdzielonych utworzonych w folderach publicznych, zadań, nadawaniem uprawnień do dostępu i współdzieleniem zasobów.  W przypadku dostarczenia oprogramowania równoważnego, należy zapewnić odpowiednie szkolenia dla liczby użytkowników odpowiadającej liczbie licencji z zakresu obsługi i eksploatacji tego oprogramowania. | |
| 2. | **Platforma systemowa:** co najmniej Windows 10/11 w wersji 32 i 64 bitowej. | |
| 3. | **Typ licencjonowania:** bezterminowe. | |