Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie

Załącznik nr 7 do SWZ

**„****OPZ Specjalistyczne oprogramowanie”**

**– szczegółowy opis przedmiotu zamówienia postępowanie na** **Zakup oprogramowania w ramach projektu „Cyfrowa Gmina” (znak sprawy: Ig.III.271.2.9.2023)**

**ZAKRES PRZEDMIOTU ZAMÓWIENIA**

1. Przedmiotem zamówienia jest oprogramowanie w wersji komercyjnej, które przeznaczone jest do legalnego użytku przez administrację publiczną. Zamawiający dopuszcza także oprogramowanie typu open-source, o ile może być legalnie użytkowane przez administrację publiczną zgodnie z licencją producenta.
2. Zamawiający wymaga także:
3. wieczystego charakteru dostarczonych licencji oprogramowania;
4. zapewnienia 12 miesięcznego wsparcia technicznego producenta oprogramowania lub Wykonawcy dla dostarczonego Oprogramowania.

**CZĘŚĆ NR 1** (opis na str. 3-15)

**Dostawa oprogramowania wraz z licencjami dla 70 stanowisk komputerowych wraz z wdrożeniem, służącego podniesieniu poziomu cyberbezpieczeństwa systemu informatycznego posiadanego przez Zamawiającego.**

**CZĘŚĆ NR 2** (opis na str. 1-20)

**Dostawa i wdrożenie oprogramowania do szyfrowania danych dla 40 stanowisk komputerowych.**

**CZĘŚĆ NR 3** (opis na str. 21-22)

**Dostawa systemu do zarządzania zdarzeniami (logami), gromadzącego i korelującego informacje z systemów informatycznych oraz urządzeń, w tym wdrożenie systemu oraz konfiguracja systemu uwierzytelniania użytkowników.**

CZĘŚĆ NR 4 (opis na str. 23-30)

Dostawa i wdrożenie oprogramowania służącego ochronie przed wyciekiem danych wraz z licencjami dla 40 stanowisk komputerowych.

CZĘŚĆ NR 5 (opis na str. 31-32)

**Dostawa dodatkowych licencji oprogramowania systemu operacyjnego dla dwóch serwerów posiadanych przez Zamawiającego, połączonych w klaster, umożliwiających uruchomienie 2 dodatkowych maszyn wirtualnych na serwerach działających w klastrze.**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI NR 1**

**„Dostawa oprogramowania wraz z licencjami dla 70 stanowisk komputerowych wraz z wdrożeniem, służącego podniesieniu poziomu cyberbezpieczeństwa systemu informatycznego posiadanego przez Zamawiającego”**

**1. Definicje**

Zamawiający dokonał opisu przedmiotu z wykorzystaniem następujących definicji:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Termin** | **Definicje** |
| 1 | **Aktualizacje** | Jakiekolwiek uaktualnienia Oprogramowania, dostarczone w związku z zapewnieniem Wsparcia Technicznego, w tym wydania uzupełniające, patche, zmiany, poprawki oraz inne dostosowania, w tym wskazane w OPZ, zapewniające prawidłowe korzystanie z takiego oprogramowania. |
| 2 | **Dokumentacja techniczna** | Wszelka dokumentacja dostarczona lub wykonana na podstawie Umowy w szczególności dokumentacja niezbędna do korzystania z Oprogramowania w tym techniczna oraz użytkowa. |
| 3 | **Dni robocze** | Dni od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej. |
| 4 | **Oprogramowanie** | Oprogramowanie opisane w pkt 2 OPZ. |
| 5 | **OPZ** | Niniejszy Opis Przedmiotu Zamówienia. |
| 6 | **Producent** | Producent Oprogramowania, oferowanego przez Wykonawcę. |
| 7 | **Umowa** | Umowa w sprawie zamówienia publicznego zawarta między Zamawiającym a Wykonawcą. |

**2. Przedmiot zamówienia**

1. Dostawa oprogramowania wraz z licencjami dla 70 stanowisk komputerowych wraz z wdrożeniem, służącego podniesieniu poziomu cyberbezpieczeństwa systemu informatycznego posiadanego przez Zamawiającego, wraz z zapewnieniem wsparcia technicznego dla dostarczonego Oprogramowania.
2. O ile nie zaznaczono inaczej, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
3. Zamawiający może wykonywać uprawnienia z rękojmi niezależnie od uprawnień wynikających z gwarancji jakości.
4. Wykonawca powinien posiadać status Partnera Producenta Oprogramowania   
   z zastrzeżeniem, że jeśli Producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga aby Wykonawca posiadał poziom partnerstwa nie niższy niż drugi licząc od najwyższego poziomu partnerstwa w hierarchii poziomów stosowanych przez Producenta. Wymóg ten dotyczy Wykonawcy i jego ewentualnego Podwykonawcy. Wykluczona jest sytuacja, aby tylko jeden z tych podmiotów posiadał wyżej wskazany poziom partnerstwa.
5. Oprogramowanie dostarczone przez Wykonawcę nie może naruszać bezpieczeństwa publicznego lub istotnego bezpieczeństwa publicznego państwa, mając na względzie fakt, iż Zamawiający art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa należy do Krajowego Systemu Cyberbezpieczeństwa, którego celem zgodnie z art. 3 wyżej wskazanej ustawy jest zapewnienie odpowiedniego poziomu cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych przez osiągnięcie odpowiedniego poziomu do świadczenia tych usług i obsługi incydentów. Tym samym dostarczone Oprogramowanie musi być zgodne z wymogami Krajowego Systemu Cyberbezpieczeństwa.

**3. Dostawa**

1. Dostawa ma zostać dokonana w dni robocze w godzinach od 7.30 do 15.00.
2. Dostarczone licencje na Oprogramowanie muszą obejmować dostęp do najnowszej wersji tego oprogramowania udostępnionej przez Producenta.
3. Licencje wraz z dostarczonym Oprogramowaniem muszą pochodzić z oficjalnego kanału dystrybucji ich Producenta.
4. Wykonawca jest zobowiązany do przekazania Zamawiającemu aktualnego zestawienia   
   w formacie xls wszystkich dostarczonych pozycji w zakresie Oprogramowania zawierających: oznaczenie Producenta, pełna nazwa produktu, metryka licencyjna, wersja i edycja Oprogramowania, rodzaj licencji, okres obowiązywania licencji, okres wsparcia technicznego, poziom wsparcia technicznego, cena jednostkowa netto, stawka podatku VAT, cena jednostkowa brutto.
5. Minimalne wymogi dla wsparcia technicznego.

Wykonawca zobowiązuje się dokonać dostawy Oprogramowania wraz z zapewnieniem dla Zamawiającego wsparcia technicznego dla dostarczonego Oprogramowania i wszelkich licencji udzielanych w celu wykonania umowy przez okres 12 miesięcy od dnia odbioru Oprogramowania.

1. Minimalny zakres wsparcia technicznego obejmuje:
2. dostęp za pośrednictwem serwisu www do aktualnej dokumentacji technicznej i bazy wiedzy publikowanej i udostępnianej przez Producenta;
3. dostęp za pośrednictwem www do obrazów (plików) do pobrania zawierających poprawki/aktualizacje/wersje instalacyjne Oprogramowania niezwłocznie po ich udostepnieniu przez producenta oprogramowania.

**4. Terminy realizacji.**

Wykonawca zobowiązany będzie zrealizować dostawę licencji na Oprogramowanie w terminie 14 dni od dnia zawarcia Umowy.

**5. Szkolenie**

Wykonawca w ramach realizacji przeprowadzi szkolenie personelu w trybie online. Szkolenie nie będzie trwało mniej niż 8 godzin i w razie potrzeby może być podzielone na kilka dni.

Szkolenie odbędzie się po zakończonych pracach wdrożeniowych oprogramowania u zamawiającego i ustalonym wcześniej terminie z zamawiającym (w ramach terminu realizacji całości zamówienia). Wykonawca na fakturze za realizację przedmiotu zamówienia wyodrębni koszt:

1. dostawy oprogramowania z jego wdrożeniem;
2. szkoleń przeprowadzonych dla pracowników Zamawiającego.

**6. Szczegółowe wymogi dla Oprogramowania.**

* 1. **Informacje Ogólne.**

1. Dostarczone licencje na oprogramowanie są bezterminowe.
2. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory posiadanymi przez Zamawiającego.
3. Oprogramowanie powinno móc współpracować z serwerem SQL Server 2019, SQL Server 2017, SQL Server 2016 SP3, SQL Server 2014 SP3, Oracle 19c oraz Oracle 12c R2.
4. Oprogramowanie serwera aplikacji umożliwia wysyłanie powiadomień mailowych.
5. Oprogramowanie posiada system ról, dzięki któremu jest możliwe przypisywanie wybranych grup stanowisk do poszczególnych użytkowników konsoli.
6. Wszelkie raporty, zestawienia oraz funkcje grupowe obejmują wtedy tylko w/w przypisane grupy stanowisk.
7. Oprogramowanie realizuje zarządzanie wszystkimi modułami systemu z poziomu tej samej konsoli zarządzającej.
8. Oprogramowanie agenta realizuje wszystkie wymagane funkcjonalności z poziomu jednej instancji usługi lub procesu bez wykorzystywania aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
9. Oprogramowanie pozwala na export do arkusza kalkulacyjnego dowolnego widoku konsoli administracyjnej.
10. Oprogramowanie pozwala zarządzać z jednej konsoli zarówno stacjami klienckimi, serwerami jak i urządzeniami mobilnymi z systemami operacyjnymi Android oraz iOS.
11. Oprogramowanie, niezależnie od ilości funkcjonalności lub zarządzanych urządzeń końcowych działa w oparciu o jedno oprogramowanie typu Agent na urządzeniu końcowym.
12. Oprogramowanie posiada architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta.
13. Oprogramowanie działa na minimalnych wymaganiach wynikających ze specyfikacji sprzętu i oprogramowania posiadanych przez Zamawiającego:

1) wymagania sprzętowe:

1. procesor minimum 2 rdzenie;
2. 8 GB wolnej pamięci- rekomendowane 16 GB;
3. karta sieciowa min 1 Gigabit;
4. przestrzeń w celu instalacji: minimum 5 GB;

2) wymagane oprogramowanie dla Serwera:

1. Serwer OS – zgodny z Windows Server 2019 (64-Bit);
2. od 5 GB wolnej przestrzeni dyskowej na instalacje serwera;
3. Baza Danych - od SQL Server 2014 SP3;

3) wymagania dla stacji klienckiej:

1. najsłabsze stacje użytkowane przez Zamawiającego są wyposażone w procesory osiągające średnią wydajność na poziomie min. 3 850 pkt w teście „PassMark - CPU Mark” według wyników opublikowanych na stronie: https://www.cpubenchmark.net;
2. od 256 MB wolnej pamięci RAM;
3. od 200 MB wolnego miejsca na dysku twardym;
4. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
5. Oprogramowanie umożliwia dystrybucję dowolnego oprogramowania, nie tylko paczek MSI, ale również takich jak InnoSetup, InstallShield i inne.
6. Oprogramowanie umożliwia automatyzowanie instalatorów wraz z możliwością customizowania instalatorów w taki sposób, żeby można było nadpisywać pola opisowe, zmieniać dowolne wartości, w tym miejsce zapisu na dysku na urządzeniu końcowym.
7. Oprogramowanie umożliwia administratorowi zautomatyzowanie procesu instalacji, w taki sposób, by nagrany został cały proces instalacji w taki sposób, by w momencie instalacji na urządzeniu końcowym nie było wymagane podanie jakichkolwiek opcji.
8. Oprogramowanie musi umożliwiać zautomatyzowania zdalnej instalacji dowolnego oprogramowania w taki sposób, by oprogramowanie można było zainstalować zdalnie w trybie cichym (Silent Mode) lub graficznym.
9. Oprogramowanie musi umożliwiać dodawanie takich opcji w instalatorach jak:
   1. blokowanie klawiatury i myszki;
   2. zmiany w ustawieniach w rejestracji na stacjach klienckich;
   3. działania na plikach i folderach na stacji klienckiej;
   4. dodanie skryptu np. w PowerShellu;
   5. zatrzymanie/wznowienie usług oraz procesów na stacji klienckiej.
10. Zdalna dystrybucja oprogramowania musi wykorzystywać natywną inteligencję instalatora. Nie może wykorzystywać Snapshotingu.
11. Zdalna dystrybucja oprogramowania musi mieć opcje Schedullingu:
12. w zadanym przedziale czasowym;
13. wprowadzenie cykliczności (np. wybrany dzień tygodnia o wybranej godzinie);
14. połączenie dwóch powyższych;
15. na żądanie w danym momencie;
16. Oprogramowanie musi umożliwiać wzbudzanie stacji klienckich metodą Wake-On-LAN.
17. Oprogramowanie musi umożliwiać administratorowi podgląd co do Statusu danego zadania per urządzenie w czasie rzeczywistym, a w przypadku błędu w wykonaniu - zwrócić informację co było przyczyną błędu.
18. W przypadku dokupienia nowych funkcjonalności/modułów oprogramowania, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
19. W przypadku zwiększenia ilości zarządzanych maszyn w dowolnym momencie, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
20. Oprogramowanie musi umożliwiać zdalną dystrybucję oprogramowania z jednej konsoli zarówno na stacjach klienckich (jak PC I laptop/notebook) jak i urządzeniach mobilnych z systemem Android i iOS.
21. Oprogramowanie dostarczy administratorowi informacji o dacie ostatniego uruchomienia aplikacji na stacji klienckiej PC per każda stacja kliencka.
22. Dystrybucja agentów na stacjach klienckich musi być możliwa zarówno w sposób automatyczny jak i ręczny.
23. Oprogramowanie umożliwia integrację z Active Directory (AD) oraz pobranie informacji z AD i automatyczne zarejestrowanie urządzeń z AD w serwerze.
24. Zarówno w przypadku stacji klienckich PC jak I urządzeń mobilnych z systemem Android oraz iOS, oprogramowanie musi umożliwiać administratorowi dostarczenie użytkownikowi końcowemu interfejsu typu self-service, w którym będzie miał listę dostępnych instalatorów z możliwością ich dociągnięcia i zainstalowania; Musi istnieć możliwość automatycznej personalizacji takiej listy per grupa lub konkretne urządzenie końcowe.
25. Oprogramowanie musi posiadać otwarte API do integracji z zewnętrznymi serwerami, np. poprzez Web Service'y.
26. Oprogramowanie musi umożliwiać również tworzenie własnych skryptów, które następnie można automatycznie instalować na urządzeniach końcowych, typu stacja kliencka.
27. W przypadku automatycznej zdalnej instalacji oprogramowania na stacjach klienckich, oprogramowanie musi dać opcje tworzenia listy oprogramowania zależnego, tzn. w przypadku gdy do poprawnego działania aplikacja X wymaga instalacji aplikacji Y, Oprogramowanie musi dawać opcję ustalenia listy takiego oprogramowania zależnego na poziomie konfiguracji aplikacji X z poziomu konsoli. W przypadku dystrybucji aplikacji X, gdy na stacji klienckiej nie będzie zainstalowana aplikacja Y, serwer automatycznie wypchnie na tą stację paczkę instalacyjną aplikacji Y .
28. Oprogramowanie musi dawać administratorowi możliwość przypisywania wykonywania tasków zarówno na urządzeniach końcowych spełniających wybrane warunki dynamiczne (np. Wolne miejsce na dysku C, wersja systemu operacyjnego itp.), jak i urządzeniach przypisanych do konkretnych grup, jak w AD.
29. Oprogramowanie musi posiadać środowisko skryptowe, umożliwiające tworzenie własnych skryptów i w łatwej dystrybucji skryptów z poziomu konsoli.
30. Oprogramowanie musi posiadać możliwość automatycznego skanowania komputerów   
    i serwerów pod kątem podatności i przestrzegania wytycznych dotyczących bezpieczeństwa i zgodności z wykorzystaniem standardowych zbiorów reguł, które są utrzymywane przez certyfikowane organizacje i firmy zajmujące się bezpieczeństwem cybernetycznym (proces wyszukiwania podatności musi bazować na minimum 25000 stale aktualizowanych reguł) oraz reguł definiowanych przez użytkownika.
    1. **Architektura Platformy.**
31. Oprogramowanie wspiera MsSQL-Server (również w wersji Express);
32. Oprogramowanie posiada konsolę zarządzającą jako część oprogramowania (nie tylko interfejs webowy);
33. Oprogramowanie posiada Agenta dla systemów klienckich Windows posiadanych przez Zamawiającego, w tym Windows oraz Windows Server;
34. Oprogramowanie wspiera więcej niż jeden serwer-repozytorium (DIP-Server) ;
35. Oprogramowanie wspiera PXE-Relay;
36. Oprogramowanie wspiera WakeUp-Points;
37. Oprogramowanie posiada możliwość integracji z Active Directory.
    1. **Komunikacja (server-clients).**
38. Oprogramowanie obsługuje niewielką przepustowością łącza dla kontroli agentów   
    i przesyłania informacji o statusach;
39. Oprogramowanie umożliwia indywidualną synchronizację pomiędzy pojedynczymi serwerami repozytorium (ograniczenie czasowe i przepustowości łącza);
40. Oprogramowanie posiada dostęp read-only do AD, bez rozszerzeń schematu;
41. Oprogramowanie umożliwia wybudzanie stacji klienckich Wake-On-LAN;
42. Oprogramowanie wspiera zadania/Joby Push i Pull (łącznie z Shutdown);
43. Oprogramowanie umożliwia komunikację bez konieczności zestawiania połączenia VPN z urządzeniami, które są poza siecią poprzez bramkę Proxy instalowaną w DMZ. Bramka Proxy musi stanowić integralną część Oprogramowania. Komunikacja pomiędzy bramką a agentem, jak i bramką a serwerem musi odbywać się poprzez HTTPS.
    1. **Operacje wykonywane przez Oprogramowanie.**
44. Oprogramowanie umożliwia pracę wielu administratorów równocześnie na jednej konsoli.
45. Oprogramowanie posiada wsparcie dla LAN, zdalne i OFFLINE stanowiska pracy.
46. Oprogramowania umożliwia wyświetlenie informacji i stanu/statusów dostępnych w czasie rzeczywistym ze znacznikiem czasowym.
47. W przypadku zakończenia wykonania zadania na stacji z błędem, administrator widzi w konsoli administracyjnej szczegółowe przyczyny błędu, które spowodowały niewykonanie danego zadania.
48. Komunikaty o błędach są generowane natychmiast (wraz z informacją o docelowym systemie OS).
49. Dowolnie definiowane dodatkowe pola (Variable/Zmienne) przechowywane w tej samej bazie danych (np. Informacje o gnieździe sieciowym, danych dotyczących wynajmu, informacje supportowe).
50. Rozbudowane funkcjonalności dotyczące zarządzania uprawnieniami.
51. Wsparcie dla grup dynamicznych na potrzeby indywidualnych informacji/widoku.
52. Oprogramowanie musi zawierać opcję ukrywania danych osobowych użytkowników (takich jak imię, nazwisko, login) dla wybranych administratorów.
53. Oprogramowanie musi umożliwiać przyznawanie i blokowanie dostępu do wybranej części infrastruktury oraz wybranych części funkcjonalności oprogramowania wskazanym administratorom.
    1. **Minimum możliwości w zakresie zadań jakie powinno spełniać oprogramowanie.**
54. Oprogramowanie umożliwia wysyłanie polecenia w trybie "Push".
55. Oprogramowanie umożliwia wysyłanie polecenia w trybie "Pull".
56. Oprogramowanie umożliwia wysyłanie polecenia w trybie "shutdown".
57. Oprogramowanie pozwala na indywidualną interakcję użytkownika w trakcie wykonywania zadania uruchomionego przez administratora w trybach: opóźnienie, odmowa, przypomnienie o instalacji.
58. Oprogramowanie umożliwia wysyłanie polecenia Wake-on LAN.
59. Oprogramowanie umożliwia automatyczne generowanie i wysyłanie powtarzających się zadań (recurring Jobs).
60. Oprogramowanie umożliwia uruchomienie zadania z poziomu użytkownika końcowego poprzez Kiosk samoobsługowy SelfService (dostępny przez Web).
61. Zadania mogą być inicjowane z poziomu aplikacji selfservice - konsoli Webowej.
62. Zawartość aplikacji SelfService (Kiosku) może być definiowana zarówno per User/Grupa Userów jak i per PC/Organisation Unit.

**6.6 Instalacja Oprogramowania (uwagi i wymagania minimalne).**

1. Określenie wymagań - przed przystąpieniem do instalacji programu, należy określić wymagania systemowe, w tym wersję systemu operacyjnego, ilość pamięci RAM, wolne miejsce na dysku twardym, itp.
2. Pobranie oprogramowania - po wybraniu odpowiedniej wersji oprogramowania, należy pobrać instalator z oficjalnej strony producenta.
3. Przed rozpoczęciem instalacji, należy przygotować serwer, na którym zostanie zainstalowane oprogramowanie.
4. Po pobraniu oprogramowania, należy uruchomić instalator, który przeprowadzi przez cały proces instalacji.
5. Wybór języka i lokalizacji - na początku instalacji, należy wybrać język oraz lokalizację.
6. Zaakceptowanie warunków licencji - przed kontynuowaniem instalacji, należy zaakceptować warunki licencji.
7. Wybór składników do zainstalowania – odpowiednich modułów oprogramowania.
8. Przed kontynuowaniem instalacji, należy określić ścieżkę, w której zostanie zainstalowane oprogramowanie.
9. Podczas instalacji, należy skonfigurować serwer baz danych, który będzie wykorzystywany przez oprogramowanie.
10. Skonfigurowanie połączenia z Active Directory - w przypadku integracji z Active Directory, należy skonfigurować połączenie z serwerem Active Directory.
11. Integracja z serwerem poczty elektronicznej, należy skonfigurować serwer poczty elektronicznej.
12. Przed zakończeniem instalacji, należy wybrać poziom zabezpieczeń dla oprogramowania.
13. Instalacja agenta na urządzeniu końcowym.
14. Po zakończeniu instalacji, należy przeprowadzić testy, które pozwolą na weryfikację poprawności działania oprogramowania.
15. Po pomyślnym przejściu testów, należy dostosować oprogramowanie do potrzeb i wymagań Urzędu.
16. Po wykonanych i udanych testach instalacja agenta na pozostałych urządzeniach końcowych.
17. Po zakończonej instalacji oprogramowania zostanie dostarczona klientowi dokumentacja powdrożeniowa.
    1. **Automatyczna dystrybucja poprawek dla systemów MS / Patch Management**
18. Oprogramowanie umożliwia dystrybucję poprawek systemu Windows (posiadanych przez Zamawiającego) bez używania Windows Server Update Services (WSUS);
19. Oprogramowanie umożliwia triggerowanie z poziomu WSUS;
20. Oprogramowanie umożliwia obsługę systemów operacyjnych posiadanych przez Zamawiającego: Windows 10, Windows 11, Windows Server 2019 z natywną instalacją oraz Windows Server 2022.
21. Producent oprogramowania zapewnia stały dostęp do bazy danych z poprawkami producenta oprogramowania systemowego - baza jest dostępna dla Klienta z poziomu konsoli oprogramowania w dniu jej opublikowania przez producenta.
22. Oprogramowanie umożliwia określenie ścisłych wymagań czasowych dla instalacji poprawek dla systemów operacyjnych i kontrolę tych wymagań. Oprogramowanie nie wymaga ingerencji w reguły eksploatacji serwerów, a mimo to zapewnia ich odpowiednio szybkie zamknięcie w razie luk w zabezpieczeniach;
23. Oprogramowanie pozwala administratorowi zarządzać aktualizacją systemów: możliwość sprawdzania tylko pod kątem brakujących poprawek i czy poprawki mają być od razu instalowane. Poprawki mogą być zatwierdzane automatycznie lub ręcznie. Oprogramowanie pozwala także ustalać reguły dla różnych grup w systemie IT;
24. Oprogramowania pozwala by metodą drag and drop w środowisku zgodnym z MMC określać, w jakich systemach mają być instalowane poprawki. W taki sam sposób definiowane są również automatyczne instalacje i sytuacje, w których administrator ma być wcześniej pytany o zgodę. Oprogramowanie automatycznie pobiera wszystkie poprawki Microsoft i na żądanie automatycznie je rozprowadza w infrastrukturze Klienta zgodnie z wytycznymi administratora kreator skryptów, konfiguracji pakietów i autmatyzacja dowolnych procesów/Automate i Package Studio.
25. Oprogramowanie pozwala na tworzenie plików transformacji (MST), które umożliwiają niezawodne dopasowanie do każdego MSI.
26. Oprogramowanie pozwala na tworzenie kreatora instalacji dla dowolnej aplikacji - nie wymaga paczki MSI.
27. Oprogramowanie pozwala tworzyć pakiety instalacyjne, gdzie w ramach procesu można zainstalować "n" aplikacji lub wykonać szereg dodatkowych funkcji związanych np. z inwentaryzacją.
28. Oprogramowanie umożliwia tworzenie plików sterujących (tansform).
29. Oprogramowanie pozwala na automatyzacje niemal każdego procesu wykonywanego ręcznie na komputerze.
30. Oprogramowania pozwala na proste tworzenie skryptów metodą drag and drop.
31. Oprogramowanie zawiera standardowy zestaw poleceń.
32. Oprogramowanie posiada możliwość sterowania również interfejsami niezgodnymi ze standardem (np. Java).
33. Oprogramowanie posiada pomoc kontekstową.
34. Oprogramowanie posiada tryb testowy step by step.
    1. **Moduły**

Dostarczone oprogramowanie powinno posiadać co najmniej poniższą funkcjonalność:

1. identyfikacja urządzeń SNMP, takich jak drukarki, routery, przełączniki inne urządzenia sieciowe;
2. wizualizacja topologii sieci;
3. automatyczne skanowanie sieci firmowej;
4. rejestracja zużycia energii na stanowiskach pracy;
5. automatyczne skanowanie pod kątem podatności;
6. zarządzanie natywnymi funkcjami bezpieczeństwa systemu operacyjnego;
7. automatyczne sprawdzanie zabezpieczeń ustawień konfiguracyjnych urządzenia;
8. tworzenie dokładnych kopii zapasowych dysków i ich odtwarzanie;
9. tworzenie kopii zapasowych plików, dokumentów i wpisów w rejestrze użytkowników;
10. tworzenie kopi zapasowych w postaci obrazu;
11. przegląd sprzętu, oprogramowania i dowolnych danych Urzędu w celu ich inwentaryzacji;
12. zintegrowane zarzadzanie licencjami, w tym przeprowadzanie instalacji niezauważalnie w tle;
13. automatyzacja dowolnych zadań administracyjnych.

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI NR 2**

**„Dostawa i wdrożenie oprogramowania do szyfrowania danych dla 40 stanowisk komputerowych”**

1. Konsola centralnego zarządzania musi wspierać posiadane przez Zamawiającego systemy operacyjne Microsoft Windows Server 2019 i Windows Server 2022 64-bit oraz Microsoft Windows 10/11 32-bit i 64-bit.
2. Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak SQL Server 2005, 2008 i 2012.
3. Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI.
4. Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443.
5. Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish.
6. Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.
7. Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania.
8. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła.
9. Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej:
10. ilość znaków,
11. czy hasło ma zawierać wielkie litery,
12. czy hasło ma zawierać małe litery,
13. czy hasło ma zawierać cyfry,
14. czy hasło ma zawierać znaki specjalne,
15. okres ważności,
16. ilość nieudanych logowań.
17. Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych.
18. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
19. ilość znaków,
20. czy hasło ma zawierać wielkie litery,
21. czy hasło ma zawierać małe litery,
22. czy hasło ma zawierać cyfry,
23. czy hasło ma zawierać znaki specjalne,
24. okres ważności,
25. ilość nieudanych logowań,
26. możliwość zmiany hasła.
27. Konsola centralnego zarządzania musi gromadzić informacje o:
28. nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania
29. danych,
30. dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych,
31. dacie aktywacji klienta systemu szyfrowania danych,
32. statusu szyfrowania,
33. typie urządzenia, na którym jest zainstalowany klient systemu szyfrowania danych,
34. stanie polityki,
35. wersji klienta systemu szyfrowania danych,
36. wersji systemu operacyjnego stacji roboczej,
37. użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej.
38. Konsola musi być dostępna z poziomu interfejsu WWW.
39. Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet.
40. Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych.
41. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny:
    1. instalacji klienta na stacji,
    2. zaszyfrowania/odszyfrowania stacji,
    3. wygenerowania klucza aktywacyjnego dla użytkownika,
    4. administrowania kluczami szyfrującymi,
    5. administrowania użytkownikami, którzy mają dostęp do stacji,
    6. administrowania profilem ustawień dla użytkowników,
    7. administrowania profilem ustawień dla stacji roboczych,
    8. wymuszenia zmiany hasła,
    9. zarządzania wieloma organizacjami z poziomu jednej konsoli.

# WYMAGANIA SYSTEMOWE APLIKACJI KLIENCKIEJ

System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku posiadanych przez Zamawiającego systemów operacyjnych Microsoft Windows Server 2019 i 2022 64-bit oraz Microsoft Windows 10/11 w wersji 32-bit i 64-bit.

# WYMAGANIA DOTYCZĄCE UWIERZYTELNIANIA

1. Aplikacja musi umożliwiać przetrzymywanie co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file).
2. Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem używanego przez Zamawiającego systemu Windows.

# WYMAGANIA DOTYCZĄCE USTAWIEŃ APLIKACJI KLIENCKIEJ

1. Aplikacja musi być dostępna przynajmniej w języku polskim.
2. Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób:
3. sektor po sektorze,
4. kontener.
5. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła.
6. Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami.
7. Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail.
8. Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
9. Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania.
10. Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.
11. Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania.
12. Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego.
13. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/- odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
14. Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła.
15. Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.
16. Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła.
17. Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów:
18. Guttman.
19. US Department of Defence 5220.22-M (8-306. /E).
20. US Department of Defence 5220.22-M (8-306. /E, CiE).
21. Kryptograficzne losowe dane liczbowe.
22. Aplikacja musi posiadać dedykowaną wtyczkę dla używanych przez Zamawiającego klientów pocztowych MS Outlook 2016 lub nowszych, również dostępnych z poziomu Office 365, którego zakup rozważa Zamawiający w późniejszym terminie.
23. Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego.
24. Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie.
25. Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji.
26. Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI.

# WYMAGANIA DOTYCZĄCE SZYFROWANIA

Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania:

1. AES (Rijndael).
2. Blowfish.
3. Triple DES (3DES).

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI NR 3**

**Dostawa systemu do zarządzania zdarzeniami (logami), gromadzącego i korelującego informacje z systemów informatycznych oraz urządzeń, w tym wdrożenie systemu oraz konfiguracja systemu uwierzytelniania użytkowników**

Zamawiający na potrzeby wdrożenia udostępni infrastrukturę na serwerach zwirtualizowanych lub fizycznych, wg specyfikacji uzgodnionych z Wykonawcą. Czynności związane z wdrożeniem systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja systemu przez Wykonawcę odbywać się będzie z wykorzystaniem środków komunikacji elektronicznej.

1. Funkcjonalności systemu.
   1. Monitorowanie występujących zdarzeń (logów) w trybie ciągłym.
   2. Zbieranie zdarzeń z serwerów wirtualnych, fizycznych, Active Directory, przełączników oraz innego rodzaju urządzeń, które są oraz zostaną podłączone do infrastruktury zamawiającego.
   3. Agregacja oraz korelacja logów.
   4. Wykrywanie ataków typu brute force na różne usługi.
   5. Wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu.
   6. Analiza logów w oparciu o wbudowane reguły bezpieczeństwa.
   7. Konfiguracja oprogramowania do przechowywania logów z kluczowych zasobów przez okres 24 miesięcy zgodnie z rozporządzeniem KRI §21 pkt. 4 „Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.”
   8. Panel do wyszukiwania zdarzeń.
2. Wdrożenie systemu.

Wykonawca będzie odpowiedzialny za instalację i konfigurację oraz optymalizację środowiska systemu w infrastrukturze Zamawiającego oraz opiekę serwisową i wsparcie techniczne przez okres minimum 12 miesięcy.

1. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratora (zarządzającego systemem), co najmniej w n/w zakresie:
   1. przedstawienie architektury systemu;
   2. omówienie procedur obsługi administracyjnej systemu;
   3. omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń systemu;
   4. przekazanie informacji na temat konfiguracji i zarządzania systemem;
   5. instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI NR 4

Dostawa i wdrożenie oprogramowania służącego ochronie przed wyciekiem danych wraz z licencjami dla 40 stanowisk komputerowych

1. Pełne wsparcie dla stacji roboczych z używanymi przez Zamawiającego systemami Windows 10 oraz Windows 11.
2. Serwer administracyjny musi oferować możliwość instalacji na posiadanych przez Zamawiającego systemach Windows Server 2019 i Windows Server 2022.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim lub angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP (dotyczące funkcji zapobiegania utracie danych) muszą być egzekwowane również w przypadku braku połączenia między klientem a serwerem zarządzającym.
10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych.
13. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z

wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.

1. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
2. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.
3. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
4. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
   1. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
   2. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
5. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory używaną przez Zamawiającego.
6. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
   1. logowanie oraz wylogowanie użytkownika,
   2. włączenie oraz wyłączenie stacji roboczej,
   3. blokada oraz odblokowanie stacji roboczej,
   4. przejście w stan bezczynności stacji roboczej.
7. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
8. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
9. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/ użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
10. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
11. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
12. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
13. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.
14. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
15. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
16. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
17. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania.
18. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.
19. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
20. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
21. aplikacje, z której zostały utworzone,
22. lokalizację,
23. adres URL,
24. format pliku,
25. zawartość pliku.
26. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
27. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
    1. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
    2. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
    3. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
    4. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
    5. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
    6. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
    7. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
       * Dropbox,
       * Google Drive,
       * SharePoint,
       * OneDrive Business,
       * OneDrive Personal.
    8. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
    9. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
    10. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,
    11. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,
28. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
29. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
30. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
31. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
32. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e- mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
33. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
34. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
35. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
36. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker dostępną w systemach operacyjnych używanych przez Zamawiającego. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
37. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
38. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o poniższe kategorie:
    1. numery kart kredytowych,
    2. numer PESEL,
    3. numer polskiego dowodu osobistego,
    4. polski numer paszportu,
    5. wyrażenia regularne,
    6. określone ciągi znaków,
    7. numer IBAN.
39. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
40. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).
41. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
42. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e- mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”).
43. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
44. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu firewall.
45. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania rozwiązań typu SIEM.
46. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania pocztowych klasy Enterprise lub równoważnym, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
47. Serwer administracyjny musi umożliwiać integrację z Office365, który zamierza nabyć Zamawiający w późniejszym terminie. Integracja musi pozwalać na:
    1. audyt i logowanie wiadomości e-mail,
    2. audyt i logowanie operacji na plikach,
    3. wprowadzanie polityk zabezpieczeń do wiadomości e-mail.
48. System musi umożliwiać integrację z narzędziami analitycznymi.
49. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
50. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
    1. Bezpieczeństwo danych:
51. Przegląd informacji o incydentach bezpieczeństwa.
52. Przegląd danych przychodzących.
53. Przegląd danych wychodzących.
54. Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.
55. Podłączane/odłączane urządzenia przenośne.
    1. Produktywność:
56. Przegląd informacji na temat produktywności użytkowników.
57. Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
58. Trendy.
    1. Eksploatacja sprzętu:
59. Przegląd informacji na temat eksploatacji sprzętu komputerowego.
60. Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
61. Eksploatacja drukarek.
62. Eksploatacji sieci.
63. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
64. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
65. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku edytora tekstu, który zawiera informacje nt:
66. plików przenoszonych na nośniki USB i inne urządzenia przenośne,
67. plików przesłanych za pomocą wiadomości e-mail,
68. plików przesłanych za pomocą poczty webowej,
69. plików przesłanych do Internetu,
70. plików wysłanych za pomocą komunikatorów,
71. plików przesłanych na dyski chmurowe,
72. analiza sposobu korzystania z aplikacji,
73. analiza korzystania z Internetu,
74. analiza wykorzystania portali do poszukiwania pracy.

**Instalacja oprogramowania**

1. Zamawiający udostępni gotową maszynę wirtualną z zainstalowanym systemem Windows Server w wersji wspieranej przez rozwiązanie oprogramowanie.
2. Wszystkie stacje, na których ma się odbyć wdrożenie, muszą być w domenie.
3. Klient musi zapewnić komunikację pomiędzy wdrażanymi PC, a serwerem oprogramowaniem.
4. W trakcie wdrożenia wdrażane stacje musza być włączone i będą musiały zostać ponownie uruchomione po instalacji.
5. Instalacja serwera,
6. Instalacja klientów na stacjach w trybie Enterprise,
7. Ustawienie kategorii danych w oparciu o wskazane przez klienta dane wrażliwe,
8. Ustawienie reguł DLP

5. Szkolenie

Wykonawca w ramach realizacji dostawy i wdrożenia oprogramowania przeprowadzi szkolenie administratora systemu w trybie online. Szkolenie nie będzie trwało mniej niż 8 godzin i w razie potrzeby może być podzielone na dni.

Szkolenie odbędzie się po zakończonych pracach wdrożeniowych oprogramowania u zamawiającego i ustalonym wcześniej terminie z zamawiającym.

6. Dokumentacja powdrożeniowa

Po zakończonej instalacji oprogramowania zostanie dostarczona zamawiającemu dokumentacja powdrożeniowa.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI NR 5

**Dostawa dodatkowych licencji oprogramowania systemu operacyjnego dla dwóch serwerów posiadanych przez zamawiającego, połączonych w klaster, umożliwiających uruchomienie 2 dodatkowych maszyn wirtualnych na serwerach działających w klastrze**

Zamawiający posiada następujące serwery marki DELL połączone w klaster:

1. starszy serwer Dell PowerEdge R330 z wdrożoną usługą Microsoft Active Directory na poziomie Microsoft Windows Server STD 2019;
2. nowy serwer DELL EMC R450 wraz z systemem operacyjnym Microsoft Windows Server STD 2022 16 core.

**Zamawiający wymaga dostawy oprogramowania zgodnego z oprogramowaniem posiadanym przez Zamawiającego w formie dwóch odrębnych licencji w wersji 16 core:**

1. **jedna licencja wieczysta w wersji License Pack,** która będzie zainstalowana na starszym serwerze, a z czasem będzie mogła być przeniesiona na nowy serwer, który Zamawiający zamierza zakupić w przyszłości;
2. **jedna licencja wieczysta w wersji OEM,** która będzie zainstalowana na nowym serwerze.

Obie licencje oprogramowania powinny być w najnowszej rynkowej wersji, z możliwością downgrade’u do wersji systemu posiadanego przez Zamawiającego na starszym serwerze.

Licencje równoważne w stosunku do już posiadanych przez Zamawiającego

W przypadku zaproponowania licencji równoważnych, Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 7 godzin.

Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ.

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