

Załącznik nr 7

Opis Przedmiotu Zamówienia (zwany „OPZ”)

Przedmiotem zamówienia jest dostawa oprogramowania, zasilaczy awaryjnych oraz urządzeń typu switch podnoszącego poziom Cyberbezpieczeństwa w Urzędzie Miasta i Gminy w Sobkowie i jednostkach organizacyjnych w ramach zadania „Projekt Grantowy Cyberbezpieczny Samorząd Etap IV” współfinansowanego z Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Fundusze Europejskie na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa,

Część I

Miasto i Gmina Sobków posiada licencje na oprogramowanie do backup Xopero One na 30 urządzeń końcowych oraz 2 serwery ważną do 30 września 2025. Zamówienie będzie polegać na przedłużeniu licencji do 30 czerwca 2026 r.

Część II

Miasto i Gmina Sobków posiada licencje na oprogramowanie antywirusowe Bitdefender Gravit Zone na 45 stanowisk do 26 maja 2026. Zamówienie będzie polegać na podniesieniu wersji Bitdefendera do wersji Enterprise (Ultra) do końca obowiązywania licencji.

Część III

Licencja na 35 stanowisk na okres 1 rok.

Przedmiotem dostawy jest oprogramowanie do ewidencji systemów IT, który obejmuje poniższy zakres.

1. Monitorowanie infrastruktury (bezagentowo), obejmujące serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping

wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)

wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci

wizualizacji urządzeń na mapach z funkcją siatki umożliwiającą korygowanie pozycji ikon na mapie do najbliższej linii siatki

wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.

wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku

wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie

wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny

zablokowania mapy urządzeń przed przypadkową edycją

serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów.

serwerów pocztowych: monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem) - program ma możliwość wykonywania operacji testowych - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa

monitorowania serwerów WWW i adresów URL

cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS

obsługi szyfrowania SSL/TLS w powiadomieniach e-mail

obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID

obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych

monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych - ruchu sieciowego - podłączonych stacji roboczych – graficzna prezentacja panelu switcha - ruchu generowanego przez podłączone do portów stacje robocze

serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie

wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano

zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny

wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

2. Dodatkowe wymagana w zakresie modułu inwentaryzacji:

przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,

przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,

tworzenia powiązań między zasobami a urządzeniami,

tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,

tworzenia relacji pomiędzy zasobami,

wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,

definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,

określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,

określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,

masową edycję atrybutów zasobów,

definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,

importu danych z zewnętrznego źródła (.CSV),

przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,

tworzenia powiązań między zasobami a dokumentami w relacji 1:N,

oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,

ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,

generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,

przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,

konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,

konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,

archiwizacji i porównywania audytów zasobów,

tworzenia kodów kreskowych dla zasobów,

drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
inventaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
inventaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inventaryzacji offline),
definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnięcie licencja/gwarancja”).

3. Inventaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.

Informacje o aplikacjach używanych w organizacji.

Tworzenie własnych wzorców aplikacji.

Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.

Informacje o komputerach, na których aplikacja została wykryta.

Zarządzanie posiadanymi licencjami.

Wskazywanie osób odpowiedzialnych za licencję. Wskazanie użytkowników licencji.

Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.

Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.

Zarządzanie posiadanymi licencjami: raport zgodności licencji.

Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe posiadają możliwość filtrowania elementów per oddział.

4. W zakresie obsługi użytkowników program ma umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),

Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,

Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,

Informacji o edytowanych przez użytkownika dokumentach,

Historii pracy (cykliczne zrzuty ekranowe),

Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),

Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),

Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,

Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

5. Program ponadto ma posiadać możliwość:

wykrywania podejrzanej aktywności przez popularne „jiggler”, mającej na celu symulowanie faktycznej pracy.

zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.

wyszczególnienia podejrzanej aktywności w raportach.

wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl).
Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
blokowania ruchu na wskazanych portach TCP/IP,
blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
prowadzenia rejestru naruszeń blokad
wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku.
Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

6. Program, który umożliwia pomoc zdalną dla użytkowników.

W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcją odrzucenia takiego połączenia przez użytkownika (np. w przypadku pracowników wysokiego szczebla).

Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran.

Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.

W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.

Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę.

Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.

Moduł ten zawiera również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów).

Ponadto czat pozwala na:

Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.

zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej

rozmowy również między „zwykłymi” użytkownikami

osadzanie załączników w treści wiadomości,

osadzanie obrazków w treści wiadomości,

formatowanie tekstu,

tworzenie pokojów tematycznych, rozmów grupowych

oznaczanie kontaktów jako „ulubionych” na liście kontaktów

uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW helpdesku

może być wyświetlany w trybie jasnym lub ciemnym W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic).

Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz linkami do artykułów w bazie wiedzy.

Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta.

Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.

Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. Moduł pomocy zdalnej umożliwia również:

pobieranie listy użytkowników z Active Directory wraz z awatarami,

wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, | zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, | zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, | zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,

zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,

tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,

automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,

definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,

przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,

procesowanie zgłoszeń użytkowników z wiadomości e-mail

dostęp do plików źródłowych wiadomości e-mail przetworzonych na zgłoszenia,

obsługę wielu adresów e-mail jednego użytkownika w celu przetwarzania jako zgłoszeń pochodzących od tej samej osoby,

eksportowania listy zgłoszeń do plików CSV i XLSX,

integrację ze wieloma skrzynkami e-mail w celu obsługi różnych kanałów zgłoszeń wraz z automatyzacjami,

integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,

tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,

wykonywanie operacji na wielu zgłoszeniach równocześnie,

dołączanie załączników do zgłoszeń,

usuwanie zamkniętych zgłoszeń,

rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,

szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,

wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,

zrzuty ekranowe (podgląd pulpitu),
zdalną modyfikację rejestrów, dystrybucję oprogramowania przez Agenty,
definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecenia operacji następuje kolejgowanie zadania dystrybucji pliku,
możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
planowanie nieobecności pracowników helpdesk,
obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
generowanie raportów obsługi helpdesk,
zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

7. MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM poprzez blokowanie urządzeń.

Blokowanie urządzeń i nośników danych.

Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskiectek.

Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.

Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.

Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.

Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.

Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.

Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.

Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.

Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.

Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

8. Zarządzanie prawami dostępu do urządzeń:

Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.

Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.

Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.

Przydzielanie uprawnień również do kont użytkowników lokalnych. Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.

9. System ma wspierać zarządzanie CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania.

Dostęp realizowany jest przez przeglądarkę internetową a strona może być wyświetlana w trybie jasnym lub ciemnym.

Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.

Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.

Statystyki aktywności podwładnych widoczne dla przełożonego.

Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.

Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.

Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.

Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.

Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.

Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.

Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).

Wskaźnik czasu poświęconego na aktywność produktywną.

Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.

Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.

Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

10. Portal informacyjny w formie platformy WWW

Oprogramowanie posiada również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, których nazwy można zmieniać wg potrzeb. Na każdym z dashboardów widgety są rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być:

Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.

Wyświetlana w trybie jasnym lub ciemnym (nocnym). Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego. Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania:

Mapa sieci,

Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,

Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,

Statystyki z obszaru wydruków, Statystyki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad,

Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,

Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych,

Produktywność dla grupy, Statystyki czasu nieproduktywnego. Ochrona przed usunięciem Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

Funkcjonalność Agenta Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

Zabezpieczenia Instalator programu jest zabezpieczony podpisem cyfrowym wystawionym i zweryfikowanym przez zaufany globalny urząd certyfikacji (CA).

Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji. Program dostępny jest w języku polskim, angielskim, bułgarskim i litewskim, wraz z podręcznikiem Użytkownika w formie strony internetowej. Wsparcie techniczne świadczone jest telefonicznie lub mailowo w języku polskim lub angielskim.

Część IV

Wymagania Minimalne

UPS typ 1 Liczba sztuk 28	Moc całkowita 360W Moc Pozorna 600VA Czas przełączenie w tryb zasilania akumulatorowego 2-6 mili sekund. Możliwość zarządzania zasilaczem ups gniazda schuko Liczba gniazd minimum 3
UPS typ 2 liczba sztuk: 5	Moc pozorna 2000VA-3000VA Moc 2700W Czas przełączenie w tryb zasilania akumulatorowego 2-6 mili sekund. Możliwość zarządzania zasilaczem ups gniazda IEC320 ilość gniazd minimum 6 w UPS powinna znajdować się karta sieciowa
Switch 48 portów	Typ : przełącznik sieciowy zarządzalny, Standard RACK Interfejsy 48 x 10/100/1000 Base-T PoE 4 x 10 Gigabit Ethernet w tym 2 x 10G SFP+ Obsługa standardów IEEE 802.3 10BASE-T Ethernet (twisted-pair copper) IEEE 802.3u 100BASE-TX Fast Ethernet (twisted-pair copper) IEEE 802.3ab 1000BASE-T Gigabit Ethernet (twisted-pair copper) IEEE 802.3az Energy-Efficient Ethernet (EEE) IEEE 802.3x Flow Control IEEE 802.3ae 10 Gigabit Ethernet IEEE 802.3af/at Zdolność przełączania Co najmniej 176Gbps Tablica adresów MAC Co najmniej: powyżej 16 000 wejść/urządzenie Statyczne adresy MAC Co najmniej: powyżej 256 wejść Standardy POE: IEEE802.3at, IEEE802.3af

Switch	<p>Typ przełącznika</p> <p>Zarządzany</p> <p>Warstwa przełącznika Warstwa przełącznika</p> <p>L3</p> <p>Porty i interfejsy</p> <p>Podstawowe przełączanie RJ-45 Liczba portów Ethernet</p> <p>8</p> <p>Podstawowe przełączania Ethernet RJ-45 porty typ</p> <p>10G Ethernet (100/1000/10000)</p> <p>Ilość portów Fast Ethernet (copper) : 1</p> <p>Liczba portów SFP Combo : 4</p> <p>Port konsoli : RJ-45</p> <p>Liczba portów USB 2.0 :1</p> <p>Złącze zasilania</p> <p>Gniazdo wejściowe AC</p> <p>Sieć</p> <p>Obsługa 10G : Tak</p> <p>Przesyłanie danych</p> <p>Przepustowość routowania/przełączania : 240 Gbit/s</p> <p>Przepustowość: 120000 Mpps</p> <p>Prędkość przekazywania: 178 Mpps</p> <p>Rozmiar tablicy MAC</p> <p>16 000</p>
--------	--

Część V

Przedmiotem zamówienia wdrożenie, konfiguracja oprogramowania SIEM Wazuh oraz szkolenie administratora z obsługi. Oprogramowanie należy skonfigurować na 35 urządzeniach. Szkolenia musi zawierać zagadnienia z instalacji serwera wazuh, instalacji na urządzeniach końcowych, tworzenia nowych reguł i wysłania reguł na agentów na urządzeniach końcowych.