

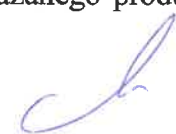
OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy zamówienia publicznego pn.:

„Zwiększenie cyberbezpieczeństwa i rozwój e-usług w Gminie Łobżenica w ramach projektu „Cyfrowa Gmina”

I. Ogólne warunki realizacji zamówienia dla każdej z części

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
7. Materiały lub urządzenia, oprogramowania pochodzące od konkretnych producentów określają minimalne parametry jakościowe, cechy użytkowe jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby spełnione zostały wymagania stawiane przez Zamawiającego. Materiały i urządzenia pochodzące od konkretnych producentów stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia.
8. Pod pojęciem „minimalne parametry jakościowe i cechy użytkowe” Zamawiający rozumie wymagania dotyczące materiałów lub urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami produktów/producentów ma wyłącznie charakter przykładowy. Zamawiający wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt w opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach użytkowych i cechach jakościowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach.



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

9. W każdym przypadku gdy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, dopuszcza rozwiązania równoważne opisywanym.

II. Zestawienie rzeczowo – ilościowe dla każdej z części

| Lp. | Nazwa | jednostka | Część postępowania |
|-----|---|-----------|--------------------|
| 1. | Doposażenie serwerowni – zakup serwera z licencją | 1 sztuka | I |
| 2. | Doposażenie serwerowni – zakup serwera z licencją | 1 sztuka | |
| 3. | Doposażenie serwerowni – zakup serwera NAS | 1 sztuka | |
| 4. | Doposażenie serwerowni – zakup routera UTM | 1 sztuka | |
| 5. | Stacje robocze | 8 sztuk | II |
| 6. | Zakup licencji oprogramowania | 78 sztuk | |
| 7. | Zakup licencji oprogramowania MS Office | 2 sztuk | |
| 8. | Stacje robocze | 17 sztuk | |
| 9. | Zakup specjalistycznego oprogramowania | 1 komplet | III |



III. Opis przedmiotu zamówienia dla Części I

Serwer z licencją (I)

| LP | Parametr lub warunek | Minimalne wymagania |
|----|----------------------------|--|
| 1 | Obudowa | -Typu Rack, wysokość maksimum 1U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack; -Możliwość instalacji ramienia porządkującego ułożenie przewodów; -Możliwość montażu ramki na froncie obudowy serwera zabezpieczającej dyski przed nieuprawnionym wysunięciem; |
| 2 | Płyta główna | -Dwuprocessorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych; -wyposażona w minimum 32 gniazda pamięci RAM DDR4, obsługa do 4000GB pamięci RAM DDR4 3200 MHz i do 10000GB pamięci RAM DDR4 i Optane PMem -Minimum 4 złącza PCI Express generacji 4, w tym minimum 3 złącza o prędkości x16; -Wszystkie złącza PCI Express muszą być aktywne; -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klitek dla dysków hot-plug; |
| 3 | Procesory | Zainstalowane dwa procesory 8-rdzeniowe w architekturze x86, osiągające wynik w testach wydajności SPECrate2017_int_base min. 123 pkt. przy konfiguracji z dwoma procesorami dla dowolnej platformy dwuprocessorowej producenta serwera, który jest oferowany w postępowaniu przez oferenta. Wymagamy aby był załączony PDF ze strony spec.org i poświadczony przez producenta serwera oferowanego w postępowaniu; Nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych; |
| 4 | Pamięć RAM | -Zainstalowane 128 GB pamięci RAM typu DDR4 Registered, 3200Mhz w kościach o pojemności 32GB; -Wsparcie dla technologii zabezpieczania pamięci ECC, Memory Scrubbing, SDDC lub równoważnej; -Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM (memory mirror); |
| 5 | Kontrolery dyskowe, I/O | -Zainstalowany kontroler SAS 3.0 obsługujący poziomy RAID 0,1,5,10 |
| 6 | Dyski twarde | -Zainstalowane 4 dyski SAS 12 Gb o pojemności 1,2 TB 10K RPM -Minimum 8 wnęk dla dysków Hotplug 2,5 cala; |
| 7 | Inne napędy zintegrowane | -Możliwość wyposażenia serwera w wewnętrzny napęd optyczny; |
| 8 | Kontrolery LAN | -Karta sieciowa wyposażona w 2 porty 10 Gbit/s Base-T -Dodatkowa osobna karta sieciowa LAN, 4x1Gbit/s RJ-45, niezajmująca slotu PCI Express (dopuszcza się instalację w slotcie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express); -Możliwość instalacji dodatkowej karty sieciowej niezajmującej slotu PCI Express; |
| 9 | Kontrolery I/O FC/SAS/Inne | -Brak |
| 10 | Porty | -zintegrowana karta graficzna ze złączem VGA z tyłu serwera; -2x USB 3.0 dostępne na froncie obudowy -2x USB 3.0 dostępne z tyłu serwera -1x USB 3.0 wewnątrz serwera Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; |
| 11 | Zasilanie, chłodzenie | -Redundantne zasilacze hotplug o mocy maksymalnej 500W każdy, o sprawności 94% (tzw klasa Platinum); -Redundantne wentylatory hotplug; -Serwer dostarczony wraz z dwoma kablami C13-C14 o długości min. 4m każdy; |
| 12 | Zarządzanie | -Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zarządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera. Wymaga się aby system rozpoznawania awarii był niezależny od zasilania i działał (wskazywał uszkodzony element) po odłączeniu kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym).

-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
- Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
- Dostęp poprzez przeglądarkę Web
- Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii
- Zarządzanie alarmami (zdarzenia poprzez SNMP)
- Możliwość przejścia konsoli tekstowej
- Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
- Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera)
- Możliwość pobrania darmowego oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera, umożliwiającego konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
- Zainstalowana, dedykowana dla potrzeb karty zarządzającej pamięć flash o pojemności minimum 16 GB;
- Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB);
- Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania;
- Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkownika zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji;
- Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń);
- Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | |
|----|---------------|---|
| | | <p>od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą;</p> <ul style="list-style-type: none"> • karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiegokolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; |
| 13 | Wspieranie OS | - Windows Server 2016, Windows Server 2019, Windows Server 2022, Oracle Linux 7.9, Oracle Linux 8.4, RedHat 7.9, RedHat 8.5, Suse 15 SP3, VMWare 6.7 U3, VMware 7.0 U2; |
| | | |

| | | |
|----|--------------------|--|
| 14 | Gwarancja | <p>-3 lat gwarancji producenta serwera w trybie onsite z czasem reakcji w miejscu instalacji serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki;</p> <p>-Dostępność części zamiennych co najmniej przez 5 lat od momentu zakupu serwera;</p> <p>-Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;</p> <p>-Wymagana możliwość automatycznego powiadamiania o awarii serwera centrum serwisowego producenta. Jeżeli funkcja taka jest płatna należy ten koszt uwzględnić w ofercie.</p> |
| 15 | Dokumentacja, inne | <p>-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dostarczone przed odbiorem).</p> <p>-Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Unii Europejskiej. Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;</p> <p>-Oferent zobowiązany jest dostarczyć przed odbiorem kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu w języku polskim lub angielskim;</p> <p>-Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801,) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;</p> <p>-Wymagane jest oświadczenie dostawcy oferowanego serwera, iż wymagany w postępowaniu poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez dostawcy serwera na potrzeby oferty w niniejszym postępowaniu;</p> <p>-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;</p> <p>-Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia. Zamawiający nie dopuszcza dostosowywania funkcji na potrzeby niniejszego postępowania.</p> <p>- Wszystkie parametry i funkcje oferowanego serwera ogólnodostępnej producenta. Wraz z serwerem należy dostarczyć licencję na OS Windows w wersji 2022 pozwalająca uruchomić taki OS na serwerze z powyżej specyfikacji.</p> |

u

Serwerowy system operacyjny

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

- 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
- 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
- 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
- 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 - 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
- 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- 10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji
- 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
- 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 - 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
- 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
- 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
- 18) Mechanizmy logowania w oparciu o:
- Login i hasło,
 - Karty z certyfikatami (smartcard),
 - Wirtualne karty (logowanie w oparciu o certyfikat chroniony przez moduł TPM),
- 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych
- 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- 22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- 23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
- 24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- 25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
- a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
 - c) Zdalna dystrybucja oprogramowania na stacje robocze.
 - d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji robocze

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
- Dystrybucję certyfikatów poprzez http
 - Konsolidację CA dla wielu lasów domeny,
 - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- f) Szyfrowanie plików i folderów
- g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
- i) Serwis udostępniania stron WWW.
- j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
- k) Wsparcie dla algorytmów Suite B (RFC 4869),
- l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
- i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - iii. Obsługi 4-KB sektorów dysków
 - iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
 - v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- 27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- 28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- 29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- 30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
- 31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim
- 32) Serwerowy system operacyjny w najnowszej wersji producenta oprogramowania dostępnej na rynku.

Serwer NAS

| Specyfikacja sprzętowa | |
|--|---|
| Procesor | Procesor 64 bit x86 o takowaniu nie mniejszym niż |
| Procesor liczba rdzeni | 2.2 GHz Nie mniej niż 4 |
| Pamięć RAM | Nie mniej niż 8GB |
| Pamięć RAM liczba slotów | Minimum 2 sloty |
| Pamięć RAM - możliwość | Nie mniej niż do 64GB |
| rozszerzenia Pamięć Flash | Nie mniej niż 5 GB |
| Liczba zatok na dyski | Minimum 4 zatoki 3,5" |
| Obsługiwane dyski | 3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" |
| Wbudowane w urządzenie interfejsy na dyski M2 | SATA SSD Wymagane min. 2 x M2 PCIe Gen3x1 |
| Możliwość stosowania dysków twardej o | do 18TB |
| Możliwość podłączenia modułu rozszerzającego | Tak, co najmniej 2 |
| Porty LAN 2,5 GbE | Minimum 2 RJ-45 |
| Diody LED | Minimum Status, LAN, HDD |
| Porty USB 3.2 Gen2 | Minimum 3 |
| Port PCIe | Tak, minimum 2 Gen3x4 |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|---------------------------------------|------------------|
| Przyciski | Reset, Zasilanie |
| Typ obudowy | Tower |
| Dopuszczalna temperatura pracy | od 0 do 40°C |
| Wilgotność względna | 5-95% R.H. |
| Zasilanie | Max. 250 W |

| Specyfikacja oprogramowania | |
|---|---|
| Obsługa dwóch systemów operacyjnych | Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS |
| Wymagania dla systemu operacyjnego opartego o system plików EXT4 | |
| Agregacja łączy Obsługiwane | Tak |
| systemy plików | Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, |
| Możliwość podłączenia karty WLAN | HFS+, exFAT Tak |
| na USB Szyfrowanie udziałów | Tak, min AES 256 |
| Szyfrowanie dysków zewnętrznych | Tak |
| Zarządzanie dyskami | Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek |
| Wbudowana obsługa iSCSI | Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| Zarządzanie prawami dostępu | Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL |
| Obsługa Windows AD | Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP |
| Funkcje backup | Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, |
| Współpraca z zewnętrznymi dostawcami usług chmury | Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box |
| Darmowe aplikacje na urządzenia mobilne | Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android |
| Minimum obsługiwane serwery | Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu |
| VPN | VPN client / VPN server Obsługa PPTP, OpenVPN |
| Administracja systemu | Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|---|---|
| | <p>Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń</p> <p>System plików dziennika</p> <p>Całkowity rejestr systemowy (poziom pliku)</p> <p>Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line</p> <p>Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie</p> |
| Wirtualizacja | <p>Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.</p> <p>Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5</p> <p>Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.</p> |
| Konteneryzacja | <p>Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker</p> |
| Zabezpieczenia | <p>Filtracja IP</p> <p>Ochrona dostępu do sieci z automatycznym blokowaniem</p> <p>Połączenie HTTPS</p> <p>FTP z SSL/TLS (Explicit)</p> <p>Obsługa SFTP (tylko admin)</p> <p>Szyfrowanie AES 256-bit</p> <p>Szyfrowana zdalna replikacja (Rsync poprzez SSH)</p> <p>Import certyfikatu SSL</p> <p>Powiadomienia o zdarzeniach za pośrednictwem Email i SMS</p> |
| Możliwość instalacji dodatkowego oprogramowania | <p>Tak, sklep z aplikacjami; możliwość instalacji z paczek</p> |
| Gwarancja | <p>3 lata</p> |
| <p>Do w/w sprzętu należy dostarczyć cztery dyski o min. następujących parametrach:</p> <ol style="list-style-type: none"> 1. Pojemność: min. 6TB 2. Prędkość obrotowa: min. 5400 RPM 3. MTBF: min. 1 mln h 4. Gwarancja: min. 3 lata (w ramach gwarancji uszkodzony dysk pozostaje własnością Zamawiającego i nie podlega zwrotowi. Wykonawca dostarczy sprawny dysk w czasie trwania gwarancji). | |

Router UTM

| Nazwa | Opis przedmiotu zamówienia |
|--|--|
| Wymagania Ogólne | <p>Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. |
| Redundancja, monitoring i wykrywanie awarii | <ul style="list-style-type: none"> - W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. - Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. - Monitoring stanu realizowanych połączeń VPN. - System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
| Interfejsy, Dysk, Zasilanie: | <ol style="list-style-type: none"> 1. System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q 4. System musi być wyposażony w zasilanie AC. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|---|---|
| <p>Parametry wydajnościowe:</p> | <ol style="list-style-type: none"> 1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbp 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – min. 700 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – min. 600 Mbps. |
| <p>Funkcje Systemu Bezpieczeństwa:</p> | <p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> 1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. |
| <p>Polityki, Firewall</p> | <ol style="list-style-type: none"> 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ol style="list-style-type: none"> a. Translację jeden do jeden oraz jeden do wielu. b. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|---|--|
| | <ol style="list-style-type: none"> 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. <ol style="list-style-type: none"> a. Amazon Web Services (AWS). b. Microsoft Azure c. Google Cloud Platform (GCP). d. OpenStack <p>Vmware NSX</p> |
| <p>Połączenia VPN</p> | <ol style="list-style-type: none"> 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: <ol style="list-style-type: none"> a. Wsparcie dla IKE v1 oraz v2. b. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). c. Obsługa protokołu Diffie-Hellman grup 19 i 20 d. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. e. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. i. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: <ol style="list-style-type: none"> a. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. b. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. c. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |
| <p>Routing i obsługa łączy WAN</p> | <ol style="list-style-type: none"> 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: <ol style="list-style-type: none"> a. Routingu statycznego. b. Policy Based Routingu. c. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|------------------------------|--|
| Funkcje SD-WAN | <ol style="list-style-type: none"> 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. |
| Zarządzanie pasmem | <ol style="list-style-type: none"> 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Ochrona przed malware | <ol style="list-style-type: none"> 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 21). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencją upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. |
| Ochrona przed atakami | <ol style="list-style-type: none"> 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| Kontrola aplikacji | <ol style="list-style-type: none"> 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|---|
| | <ol style="list-style-type: none"> 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| <p>Kontrola WWW</p> | <ol style="list-style-type: none"> 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |
| <p>Uwierzytelnianie użytkowników w ramach sesji</p> | <ol style="list-style-type: none"> 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: <ol style="list-style-type: none"> a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| <p>Zarządzanie</p> | <ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--------------------------------|---|
| | <ol style="list-style-type: none"> 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| Logowanie | <ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. |
| Certyfikaty | <ol style="list-style-type: none"> 1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: <ol style="list-style-type: none"> a. ICSA lub EAL4 dla funkcji Firewall. |
| Serwisy i licencje | <ol style="list-style-type: none"> 1. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: <ol style="list-style-type: none"> a. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy. |
| Gwarancja oraz wsparcie | <ol style="list-style-type: none"> 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|----------------------------------|--|
| Opisy do wymagań ogólnych | <ol style="list-style-type: none"> Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. Ww. dokumenty wymagane będą najpóźniej w dniu dostarczenia sprzętu |
|----------------------------------|--|

Serwer z licencją (II)

| LP | Parametr lub warunek | Minimalne wymagania |
|----|----------------------|--|
| 1 | Obudowa | <ol style="list-style-type: none"> Typu Tower; 4U; Obudowa musi umożliwiać konwersję do rack jedynie poprzez dodanie elementów fabrycznych producenta serwera (np. szyny rack czy tzw. „conversion-kit”; Maksymalna wysokość serwera po konwersji do rack - 4U; Obudowa musi posiadać fabryczne zabezpieczenie klatek z dyskami oraz napędami przed nieautoryzowanym dostępem (zamek); |
| 2 | Płyta główna | <ol style="list-style-type: none"> Wyprodukowana i zaprojektowana przez producenta serwera; Minimum 4 złącza PCI Express w tym minimum 2 złącza PCI Express 4.0 x8; Minimum 2 sloty dla dysków M.2 na płycie głównej nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slotcie M.2 bez zajmowania klatek dyskowych serwera) Zainstalowany moduł TPM 2.0. |
| 3 | Procesory | <ol style="list-style-type: none"> Zainstalowany procesor 8-rdzeniowy w architekturze x86 osiągający w oferowanym serwerze w testach wydajności SPECrate2017_int_base min. 69 pkt; Wymagane dołączenie do oferty pełnego protokołu testów SPEC dla oferowanego modelu serwera wyposażonego w oferowany procesor, protokół poświadczony przez producenta serwera; |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | |
|----|---------------------------------|--|
| 4 | Pamięć RAM | 1.Zainstalowane 32 GB pamięci RAM DDR4 3200Mhz w kościach o wielkości 16GB; 2.Wsparcie dla technologii zabezpieczania pamięci ECC; 3.Minimum 4 gniazda pamięci RAM, obsługa minimum 128GB pamięci RAM; |
| 5 | Kontrolery dyskowe, I/O | 1.Zainstalowany kontroler RAID SATA (Software) obsługujący poziom RAID 0,1,10; 2.Oferowany model serwera musi umożliwiać opcjonalną instalację wewnętrznego napędu LTO SAS zamiast napędu optycznego) |
| 6 | Dyski twarde | -Zainstalowane 2 dyski SATA 6G o pojemności 2 TB każdy, 7,2k RPM 3,5”, dyski Hotplug; -Minimum 4 wnęki dla dysków twardych Hotplug 3,5” w dostarczonej konfiguracji; -Możliwość rozbudowy serwera do obsługi co najmniej 8 dysków twardych Hotplug 3,5” |
| 7 | Inne napędy zintegrowane | -Zainstalowany wewnętrzny napęd DVD-RW -Możliwość instalacji wewnętrznego streamera LTO; |
| 8 | Kontrolery LAN | 2x 1Gb/s LAN, ze wsparciem iSCSI, RJ-45; |
| 10 | Porty | -.zintegrowana karta graficzna ze złączem VGA lub Display port; -10x USB, w tym minimum 3 złącz w standardzie USB 3.2 Gen2x1 TYP A (2 na panelu tylnym); -Możliwość wyposażenia w port RS-232-C; |
| 11 | Zasilanie | 1.Zainstalowany jeden zasilacz hotplug o sprawności 94% (tzw klasa Platinum) o mocy minimalnej 500W; 2.Możliwość wyposażenia serwera w drugi zasilacz zapewniający redundancje. |
| 12 | Zarządzanie | 1.Wbudowane diody informacyjne informujące o stanie serwera – minimum sygnalizacja (poprawna praca/usterka) dla komponentów jak: procesor, wentylatory, dyski twarde, temperatura wewnątrz obudowy, pamięci, zasilaczy; sygnalizacja pracy (zasilania), sygnalizacja identyfikacji (włączana zdalnie) 2.Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: <ul style="list-style-type: none"> • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejścia konsoli tekstowej • Opcjonalne przekierowania konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) |
| 13 | Wspierane OS | 1.Windows Server 2019, 2022, 2.SUSE Linux Enterprise Server 15 SP3, 15 SP4, |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | |
|----|---------------------------|---|
| | | 3.RHEL 8.4, 8.5, 8.6 |
| 14 | System Operacyjny | 1. Wraz z serwerem należy dostarczyć Windows Server 2022 Essentials 10-Core. |
| 15 | Gwarancja | <p>1. 1 rok gwarancji producenta serwera w trybie onsite</p> <p>2. Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;</p> <p>3. Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;</p> <p>4. Zgłoszenia serwisowe w języku polskim na dedykowany nr infolinii serwisowej producenta serwera;</p> <p>5. w ofercie należy zamieścić stronę www producenta serwera (link), pod którą Zamawiający odnajdzie: nr tel. zgłoszeń serwisowych, adres email zgłoszeń serwisowych, formularz online zgłoszeń serwisowych producenta serwera. Nie dopuszcza się stron www podmiotów trzecich oraz nr kontaktowych/email/formularzy podmiotów trzecich.</p> <p>6. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera</p> |
| 15 | Dokumentacja, inne | <p>1. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie dostawcy serwera potwierdzające spełnienie wymagań dołączone do oferty).</p> <p>2. Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;</p> |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

IV. Opis przedmiotu zamówienia dla Części II

Stacje robocze (I)

| Podzespól | Opis |
|------------------------------------|--|
| Typ komputera | Komputer stacjonarny (8sztuk) |
| Procesor | Procesor klasy x86, min. sześciordzeniowy, umożliwiający osiągnięcie przez oferowany zestaw w teście PassMark CPUMark wyniku średniego 19400 punktów wg strony https://www.cpubenchmark.net/cpu_list.php |
| Płyta główna | Chipset współpracujący z procesorami wielordzeniowymi wspierający pamięci DDR4, Typ podstawki: dedykowany dla procesora Min. jedno gniazdo PCI-Ex16, min. jedno gniazdo PCI-E x1 Min. 12 x USB, Min 4 x SATA III Min 1 x M.2 slot (Key M) z obsługą dysków PCIe x4 i/lub SATA 6Gb/s 2260/2280 |
| Pamięć operacyjna | Pamięć RAM 8 GB DDR4 w jednym module, z możliwością rozbudowy do 64GB |
| Porty w tylnej części komputera | Komputer wyposażony w następujące gniazda na tylnym panelu I/O: <ul style="list-style-type: none"> • co najmniej 1 gniazdo PS/2 do obsługi myszki i klawiatury • co najmniej 4 gniazda USB 2.0 • co najmniej 2 gniazda USB 3.2 • 1 gniazdo portu LAN RJ-45 • gniazda DisplayPort, HDMI, DVI, D-Sub • Zestaw gniazd audio wielokanałowej karty dźwiękowej |
| Porty w przedniej części komputera | Komputer wyposażony w następujące gniazda na przednim panelu obudowy <ul style="list-style-type: none"> • 2 gniazda USB 3.2 i min 2 gniazda USB 2.0 • 1 gniazdo do przyłączenia słuchawek i 1 gniazdo do przyłączenia mikrofonu; |
| Dysk twardy | Dysk SSD 256 GB SATA |
| Napęd optyczny | Nagrywarka DVD+/-RW DL |
| Karta graficzna | Zintegrowana z płytą główną, pozwalająca na osiągnięcie rozdzielczości min. 4096 x 2160, umożliwiająca osiągnięcie w teście PassMark 3GD Mark wyniku średniego min. 1600 punktów wg strony: https://www.videocardbenchmark.net , złącza 1xDSub, 1xDP, 1xDVI-D, 1xHDMI |
| Karta sieciowa | Zintegrowana z płytą główną, o prędkości 10/100/1000Mb/s. |
| Karta dźwiękowa | Zintegrowana z płytą główną |
| BIOS | <ul style="list-style-type: none"> - BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera wraz z datą kompilacji BIOS, |

Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia Program Operacyjny Polska Cyfrowa na lata 2014 – 2020

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|-------------------|--|
| | <p>ilości i sposobu obłożenia slotów pamięciami RAM, typie procesora wraz z informacją o ilości rdzeni, pojemności zainstalowanego dysku twardego rodzajach napędów optycznych MAC adresie zintegrowanej karty sieciowej kontrolerze audio</p> <ul style="list-style-type: none"> - Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) - Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń - Możliwość polegająca na kontrolowaniu urządzeń wykorzystujących magistralę komunikacyjną PCI, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych. Pod pojęciem kontroli Zamawiający rozumie funkcjonalność polegającą na blokowaniu/odblokowaniu slotów PCI. - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. - Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. - Możliwość założenie szyfrowanego hasła na dysk SSD (funkcja działająca osobno i niezależnie od haseł administratora/użytkownika UEFI) oparte o standard AES256 - Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. - Możliwość selektywnego wyłączenia pojedynczych portów USB |
| Klawiatura | Klawiatura USB standard QWERTY producenta zestawu komputerowego |
| Mysz | Mysz USB optyczna z rolką producenta zestawu komputerowego |
| Obudowa | <p>Małogabarytowa typu SFF do pracy w pozycji pionowej i poziomej, o sumie wymiarów nie większej niż 82 cm, wyposażona przynajmniej w:</p> <ul style="list-style-type: none"> • 1 zewnętrzną zatokę 5,25" • 1 zewnętrzną zatokę 3,5" • 1 wewnętrzną zatokę 3,5" • Beznarzędziowe otwieranie i zamykanie • Beznarzędziowy montaż napędów, dysków i kart rozszerzeń • Złącze kensigton, zamek nie wystający poza obrys obudowy <p>Możliwość otwarcia obudowy komputera i dołożenia komponentów przez wykwalifikowany personel Zamawiającego bez utraty gwarancji.</p> |
| Zasilacz | O mocy minimalnej 300W i sprawności 80+ Bronze, wymagane potwierdzenie obecności zasilacza na stronie https://www.clearesult.com/80plus/ i dostarczenie raportu z potwierdzoną sprawnością 85% przy 50% obciążenia |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|---|---|
| Bezpieczeństwo i funkcje zarządzania | <ul style="list-style-type: none"> Możliwość zastosowania mechanicznego zabezpieczenia przed kradzieżą komputera. Możliwość zastosowania mechanicznego zabezpieczenia przed niepowołanym dostępem do wnętrza obudowy. |
| Certyfikaty i oświadczenia | <p>Certyfikat PN-EN ISO 9001:2015, PN-EN ISO14001:2015 oraz PN-ISO/IEC 27001:2014 lub nowsze na procesy projektowania, produkcję, sprzedaż i serwis, Certyfikat PN-EN ISO 50001:2018 Certyfikat SA 8000:2014 Oferowany komputer musi znajdować się na liście „Windows Hardware Compatibility List”. Wymagany wydruk ze strony oraz zawartość Windows Logo Verification Report Komputer musi być certyfikowany na zgodność z systemem operacyjnym MS Windows 11 – x64 Oznaczenie CE Oświadczenie o przejęciu serwisu przez producenta zestawu komputerowego, w przypadku nie wywiązywania się oferenta z usług gwarancyjnych. Certyfikaty wymagane do złożenia wraz z ofertą</p> |
| Instrukcja | Dla każdego zestawu w języku polskim |
| Gwarancja | Minimum 36 miesięcy |
| System operacyjny | <p>Licencja na MS Windows 11 Professional PL 64 bit OEM z nośnikiem, lub równoważny tj.:</p> <ul style="list-style-type: none"> - obsługujący wszystkie programy obsługiwane przez ww. system, - posiadający wszystkie funkcjonalności ww. systemu, - obsługujący wszystkie urządzenia obsługiwane przez ww. system, - współpracujący z usługą MS Active Directory <p>- Zamawiający dopuszcza zaoferowanie równoważnego systemu operacyjnego, który umożliwi uruchomienie i pełne wykorzystanie aplikacji firmy Microsoft w tym MS Teams, MS Word, itd. W wersjach nie starszych niż 2019.</p> <p>- Zamawiający oczekuje dostarczenia fabrycznie nowego systemu operacyjnego nieużywanego i nie aktywowanego nigdy wcześniej na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. Zamawiający nie akceptuje systemów „refurbished”. Zamawiający przewiduje możliwość weryfikacji kodów licencyjnych bezpośrednio w firmie Microsoft.</p> |
| Sterowniki | <p>Komplet sterowników do podzespołów składowych komputera na nośnikach optycznych. Możliwość ściągnięcia aktualnych sterowników z witryny producenta komputera poprzez podanie numeru seryjnego komputera – załączyć zrzut witryny producenta komputera z niniejszą funkcjonalnością.</p> |
| Wsparcie techniczne | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta – załączyć zrzut witryny producenta komputera z niniejszą funkcjonalnością. |
| | Monitor |
| Technologia wykonania matrycy | VA |
| Rozmiar plamki | Maksymalnie 0,275mm |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|-----------------------------------|---|
| Jasność | 250 cd/m² |
| Kontrast | Typowy 3000:1 |
| Kąt widzenia (pion/poziom) | 178/178 stopni |
| Czas reakcji matrycy | Max. 8ms |
| Rozdzielczość maksymalna | 1920x1080 przy 60Hz |
| Paleta kolorów | 83% (CIE 1976) |
| Głębina kolorów | 16,7 miliona kolorów |
| Zużycie energii | Maks. 28W W trybie uśpienia maks. 0,3W |
| Powłoka powierzchni ekranu | Antyodblaskowa utwardzona |
| Podświetlenie | System podświetlenia LED |
| Bezpieczeństwo | Monitor musi być wyposażony w tzw. Gniazdo zabezpieczenia przed kradzieżą. Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie. |
| Waga bez podstawy | Maksymalnie 4 kg |
| Pochylenie monitora | W zakresie min. 26 stopni |
| Kolor obudowy | Czarny |
| Złącze | 1 x D-Sub 1 x HDMI 1.4 |
| Gwarancja | Min. 3 lata, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną i stronę internetową producenta Czas reakcji serwisu – do końca następnego dnia roboczego |
| Certyfikaty | Energy Star Należy dołączyć do oferty. |
| Inne | Zdejmowana podstawa oraz otwory montażowe w obudowie VESA |

Oprogramowanie biurowe (I)

| | |
|-------------------------------|---|
| Oprogramowanie biurowe | <p>Zintegrowany pakiet aplikacji biurowych pochodzących od jednego producenta, w którego skład ma wchodzić min.:</p> <ul style="list-style-type: none"> - edytor tekstów; - arkusz kalkulacyjny; - narzędzie do przygotowania i prowadzenia prezentacji; - narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami); - pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. - powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, |
|-------------------------------|---|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|---|
| | <p>przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim.</p> <ul style="list-style-type: none">- dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego- publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu.- możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0). <p>Edytor tekstów musi umożliwiać:</p> <ul style="list-style-type: none">- Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.- Wstawianie oraz formatowanie tabel.- Wstawianie oraz formatowanie obiektów graficznych.- Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).- Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.- Automatyczne tworzenie spisów treści.- Formatowanie nagłówków i stopek stron.- Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.- Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.- Określenie układu strony (pionowa/pozioma).- Wydruk dokumentów.- Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.- Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. <p>Arkusz kalkulacyjny musi umożliwiać:</p> <ul style="list-style-type: none">- Tworzenie raportów tabelarycznych –- Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych <p>–</p> |
|--|---|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| | <ul style="list-style-type: none">- Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.- Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)- Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.- Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych –- Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych- Wyszukiwanie i zamianę danych- Wykonywanie analiz danych przy użyciu formatowania warunkowego- Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie- Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności- Formatowanie czasu, daty i wartości finansowych z polskim formatem- Zapis wielu arkuszy kalkulacyjnych w jednym pliku.- Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. <p>Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:</p> <ul style="list-style-type: none">- Przygotowywanie prezentacji multimedialnych, które mogą być prezentowane przy użyciu projektora multimedialnego- Drukowanie w formacie umożliwiającym robienie notatek –- Zapisanie jako prezentacja tylko do odczytu.- Nagrywanie narracji i dołączanie jej do prezentacji- Opatrywanie slajdów notatkami dla prezentera- Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo- Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego- Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym- Możliwość tworzenia animacji obiektów i całych slajdów- Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera <p>Narzędzie do zarządzania informacją prywatną (poczta elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <ul style="list-style-type: none">- Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, - |
|--|--|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|---|
| | <ul style="list-style-type: none"> - Przechowywanie wiadomości na serwerze lub w lokalnym pliku stworzonym z zastosowaniem efektywnej kompresji danych, - - Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, - Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, - - Automatyczne grupowanie poczty o tym samym tytule, - Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, - Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, - Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, - Zarządzanie kalendarzem, - - Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, - Przeglądanie kalendarza innych użytkowników, - Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, - Zarządzanie listą zadań, - Zlecanie zadań innym użytkownikom, - - Zarządzanie listą kontaktów, - - Udostępnianie listy kontaktów innym użytkownikom, - Przeglądanie listy kontaktów innych użytkowników, - Możliwość przesyłania kontaktów innym użytkownikom. |
|--|---|

Stacje robocze (II)

| Podzespół | Opis |
|--|---|
| Typ komputera | Komputer stacjonarny – 17szt. |
| Procesor | Procesor klasy x86, min. sześciordzeniowy, umożliwiający osiągnięcie przez oferowany zestaw w teście PassMark CPUMark wyniku średniego 19400 punktów wg strony http://www.cpubenchmark.net/cpu_list.php |
| Płyta główna | <ol style="list-style-type: none"> 1. Chipset współpracujący z procesorami wielordzeniowymi wspierający pamięci DDR4, 2. Typ podstawki: dedykowany dla procesora 3. Min. jedno gniazdo PCI-Ex16, min. dwa gniazda PCI-E x1 4. Min.12xUSB, 5. Min. 4 SATA III 6. Min. 1 x M.2 slot (Key M) z obsługą dysków PCIe x4 i/lub SATA 6Gb/s 2260/2280 |
| Pamięć operacyjna | Pamięć RAM 8 GB DDR4 w jednym module, z możliwością rozbudowy do 64 GB |
| Porty w tylnej części komputera | Komputer wyposażony w następujące gniazda na tylnym panelu I/O: |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|---|--|
| | <ol style="list-style-type: none"> 1. 1 gniazdo PS/2 do obsługi myszki i klawiatury 2. Co najmniej 4 gniazda USB 2.0 3. Co najmniej 2 gniazda USB 3.2 4. 1 gniazdo portu LAN RJ-45 5. Gniazda Display Port, HDMI, DP, DVI, D-Sub 6. Zestaw gniazd audio wielokanałowej karty dźwiękowej |
| Porty w przedniej części komputera | <p>Komputer wyposażony w następujące gniazda na przednim panelu obudowy</p> <ol style="list-style-type: none"> 1. 2 gniazda USB 3.2 i min. 1 gniazda USB 2.0 2. 1 gniazdo do przyłączenia słuchawek i 1 gniazdo do przyłączenia mikrofonu |
| Dysk twardy | Dysk SSD 256 GB SATA |
| Napęd optyczny | Nagrywarka DVD+/-RW DL |
| Karta graficzna | Zintegrowana z płytą główną, pozwalająca na osiągnięcie rozdzielczości min. 4096x 2160, umożliwiająca osiągnięcie w teście PassMark 3 GD Mark wyniku średniego min. 1600 punktów wg strony: https://www.videocardbenchmark.net , złącza 1xDSub, 1xDP, 1xDVI-D, 1xHDMI |
| Karta sieciowa | Zintegrowana z płytą główną, o prędkości 10/100/1000Mb/s |
| BIOS | <ol style="list-style-type: none"> 1. BIOS zgodny ze specyfikacją UEFI 2. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: Wersji BIOS Nr seryjnym komputera wraz z datą kompilacji BIOS Ilości i sposobu obłożenia slotów pamięciami RAM Typie procesora wraz z informacją o ilości rdzeni Pojemności zainstalowanego dysku twardego Rodzajach napędów optycznych MAC adresie zintegrowanej karty sieciowej kontrolerze audio 3. Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i pootrzymania BIOS) 4. Funkcja blokowania/ odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. 5. Możliwość polegająca na kontrolowaniu urządzeń wykorzystujących magistralę komunikacyjną PCI, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych. Pod pojęciem kontroli Zamawiający rozumie funkcjonalność polegającą na blokowaniu/odblokowaniu slotów PCI. 6. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość zmiany hasła pozwalającego na |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|---|--|
| | <p>uruchomieniu systemu bez podania hasła administratora.</p> <p>7. Możliwość włączenia / wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera i innych, podłączonych do niego, urządzeń zewnętrznych.</p> <p>8. Możliwość założenia szyfrowanego hasła na dysk SSD (funkcja działająca osobno i niezależnie od haseł administratora/ użytkownika UEFI) oparte o standard AES256</p> <p>9. Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne</p> <p>10. Możliwość selektywnego wyłączania pojedynczych portów USB</p> |
| Klawiatura | Klawiatura USB standard QWERTY producenta zestawu komputerowego |
| Mysz | Mysz USB optyczna z rolką producenta zestawu komputerowego |
| Obudowa | <p>Małogabarytowa typu SFF do pracy w pozycji pionowej i poziomej, o sumie wymiarów nie większej niż 82 cm, wyposażona przynajmniej w :</p> <ol style="list-style-type: none"> 1) 1 zewnętrzna zatokę 5.25” 2) 1 zewnętrzna zatokę 3,5” 3) 1 zewnętrzna zatokę 3,5 4) Beznarzędziowe otwierania i zamykanie 5) Beznarzędziowy montaż napędów dysków i kart rozszerzeń 6) Złącze kensigton, zamek nie wystający poza obrys obudowy. <p><u>Możliwość otwarcia obudowy komputera i dołożenia komponentów przez wykwalifikowany personel Zamawiającego bez utraty gwarancji.</u></p> |
| Zasilacz | <p>O mocy min. 300W i sprawności 80+Bronze, wymagane potwierdzenie obecności zasilacza na stronie https://www.clearesult.com/80plus i dostarczenie raportu z potwierdzoną sprawnością 85% przy 50% obciążenia</p> <p>Raport należy złożyć wraz z ofertą</p> |
| Bezpieczeństwo i funkcje zarządzania | <p>Możliwość stosowania mechanicznego zabezpieczenia przed kradzieżą komputera.</p> <p>Możliwość zastosowania mechanicznego zabezpieczenia przed niepowołanym dostępem do wnętrza obudowy.</p> |
| Certyfikaty i oświadczenia | <p>Certyfikat PN-EN ISO 9001:2015, PN-EN ISO14001:2015 oraz PN-ISO/IEC 27001:2014 lub nowsze na procesy projektowania, produkcję, sprzedaż i serwis,</p> <p>Certyfikat PN-EN ISO 50001:2018</p> |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--------------------------------------|--|
| | <p>Certyfikat SA 8000:2014 Oferowany komputer musi znajdować się na liście „Windows Hardware Compatibility List”. Wymagany wydruk ze strony oraz zawartość Windows Logo Verification Report Komputer musi być certyfikowany na zgodność z systemem operacyjnym MS Windows 11 – x64 Oznaczenie CE Oświadczenie o przejściu serwisu przez producenta zestawu komputerowego, w przypadku nie wywiązywania się oferenta z usług gwarancyjnych. Certyfikaty wymagane do złożenia wraz z ofertą</p> |
| Instrukcja | Dla każdego zestawu w języku polskim |
| Gwarancja | Minimum 36 miesięcy |
| System operacyjny | <ol style="list-style-type: none"> 1. Licencja na MS Windows 11 Professional PL 64 bit OEM z nośnikiem, lub równoważny tj.: <ol style="list-style-type: none"> a) obsługujący wszystkie programy obsługiwane przez ww. system, b) posiadający wszystkie funkcjonalności ww. systemu, c) obsługujący wszystkie urządzenia obsługiwane przez ww. system, d) współpracujący z usługą MS Active Directory 2. Zamawiający dopuszcza licencje typu National Academic dla edukacji. 3. Zamawiający dopuszcza zaoferowanie równoważnego systemu operacyjnego, który umożliwi uruchomienie i pełne wykorzystanie aplikacji firmy Microsoft w tym MS Teams, MS Word, itd. W wersjach nie starszych niż 2019. 4. Zamawiający oczekuje dostarczenia fabrycznie nowego systemu operacyjnego nieużywanego i nie aktywowanego nigdy wcześniej na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. Zamawiający nie akceptuje systemów „refurbished”. Zamawiający przewiduje możliwość weryfikacji kodów licencyjnych bezpośrednio w firmie Microsoft. |
| Sterowniki | <p>Komplet sterowników do podzespołów składowych komputera na nośnikach optycznych. Możliwość ściągnięcia aktualnych sterowników z witryny producenta komputera poprzez podanie numeru seryjnego komputera – załączyć zrzut witryny producenta komputera z niniejszą funkcjonalnością.</p> |
| Wsparcie techniczne | <p>Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta – załączyć zrzut witryny producenta komputera z niniejszą funkcjonalnością. Monitor</p> |
| Technologia wykonania matrycy | VA |
| Rozmiar plamki | Maksymalnie 0,275mm |
| Jasność | 250 cd/m2 |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|-----------------------------------|---|
| Kontrast | Typowy 3000:1 |
| Kąt widzenia (pion/poziom) | 178/178 stopni |
| Czas reakcji matrycy | Max. 8ms |
| Rozdzielczość maksymalna | 1920x1080 przy 60Hz |
| Paleta kolorów | 83% (CIE 1976) |
| Głębia kolorów | 16,7 miliona kolorów |
| Zużycie energii | Maks. 28W W trybie uśpienia maks. 0,3W |
| Powłoka powierzchni ekranu | Antyodblaskowa utwardzona |
| Podświetlenie | System podświetlenia LED |
| Bezpieczeństwo | Monitor musi być wyposażony w tzw. Gniazdo zabezpieczenia przed kradzieżą. Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie. |
| Waga bez podstawy | Maksymalnie 4 kg |
| Pochylenie monitora | W zakresie min. 26 stopni |
| Kolor obudowy | Czarny |
| Złącze | 1 x D-Sub 1 x HDMI 1.4 |
| Gwarancja | Min. 3 lata, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną i stronę internetową producenta Czas reakcji serwisu – do końca następnego dnia roboczego |
| Certyfikaty | Energy Star Należy dołączyć do oferty. |
| Inne | Zdejmowana podstawa oraz otwory montażowe w obudowie VESA |

Oprogramowanie biurowe (II)

MS Office 2021 Pro 64bit dla jednostek edukacyjnych lub równoważny, tj.: pakiet biurowy z kluczem licencyjnym i możliwością pobrania programu instalacyjnego ze strony producenta - umożliwiające otwarcie, edycję i zapisywanie pliku wynikowego w formatach określonych w załączniku nr 2 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247) zawierający przynajmniej edytor tekstu, arkusz kalkulacyjny, narzędzie do tworzenia prezentacji multimedialnych i klienta pocztowego.

- a. Licencja powinna być nieograniczona w czasie,
- b. Wykonawca zobowiązuje się dostarczyć niepowtarzalny (unikatowy) klucz do aktywacji dostarczonych licencji,
- c. Oprogramowanie musi być fabrycznie nowe, objęte gwarancją oraz pochodzić z autoryzowanego kanału sprzedaży na rynek Unii Europejskiej,

Oprogramowanie nie może być wcześniej używane, regenerowane, serwisowane, rejestrowane ani aktywowane – Zamawiający zastrzega sobie prawo do weryfikacji czy dostarczone oprogramowanie (licencje) i powiązane z nimi elementy, takie jak certyfikaty/etykiety dołączone do oprogramowania są oryginalne, nowe i licencjonowane zgodnie z prawem oraz zasadami producenta oprogramowania.

V. Opis przedmiotu zamówienia dla Części III

| Nazwa | Opis przedmiotu zamówienia |
|----------------------------|--|
| Ogólne: | <ol style="list-style-type: none"> 1. Oprogramowanie może być dostarczane w dwóch scenariuszach: <ul style="list-style-type: none"> • Cloud(Software as Service), • On-premise. 2. Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud. 3. Interfejs systemu dostępny jest w języku: 4. polskim 5. angielskim 6. Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych, 7. Oprogramowanie może być uruchomione w kontenerze docker. 8. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: <ul style="list-style-type: none"> ◦ Debian: 9+ ◦ Ubuntu: 16.04+ ◦ Fedora: 29+ ◦ CentOS: 7+ ◦ RHEL: 6+ ◦ openSUSE: 15+ ◦ SUSE Enterprise Linux (SLES): 12 SP2+ ◦ Windows Client: 7, 8.1, 10 (1607+) ◦ Windows Server: 2008 R2+, 9. System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji. 10. Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju). |
| Wsparcie techniczne | <ol style="list-style-type: none"> 1. Pomoc techniczna w językach: <ul style="list-style-type: none"> • Polskim • Angielski 2. Materiały samopomocowe : <ul style="list-style-type: none"> • Baza wiedzy: <ul style="list-style-type: none"> - polski - angielski |
| Zarządzanie : | <ol style="list-style-type: none"> 1. Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej. 2. Zarządzanie całym systemem poprzez dashboardy, |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| | <ol style="list-style-type: none">3. Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,4. System posiada wbudowane predefiniowane zadania backupowe,5. System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.6. Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem.7. Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem.8. Monitorowanie postępu działania zadania,9. Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:<ol style="list-style-type: none">10. zostało zakończone pomyślnie,11. Zadanie zostało zakończone z ostrzeżeniami12. Zadanie zostało zakończone z błędem13. Zadanie zostało anulowane14. Zadanie nie zostało uruchomione15. System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.16. Możliwość zdefiniowania okna backupowego dla każdego z zadań17. Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów18. System pozwala na klonowanie planów kopii zapasowych19. System umożliwia reset hasła administratora w przypadku jego utraty, Oprogramowanie umożliwia definiowanie retencji według schematów:<ul style="list-style-type: none">• GFS(Grandfather-Father-Son),• FIFO(First-In, First-Out20. Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami.21. Konta użytkowników mogą być tworzone poprzez import pliku CSV, Oprogramowanie umożliwia tworzenie grup urzędzeń Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów) |
|--|--|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|----------------------------------|---|
| | <p>22. System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:</p> <ul style="list-style-type: none"> • System Administrator • Backup operator • Viewer |
| <p>Składowanie danych</p> | <ol style="list-style-type: none"> 1. Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie 2. System umożliwia składowanie danych: <ul style="list-style-type: none"> • Lokalnie: <ul style="list-style-type: none"> - zasób SMB - zasób NFS - zasób ISCSI - zasób S3 - katalog zabezpieczonego urzędu • W chmurze : <ul style="list-style-type: none"> - Amazon Web Service - magazyn zgodny z S3 - dostarczanej przez producenta 3. System pozwala na zdefiniowanie zapasowej ścieżki repozytorium , na wypadek niedostępności głównej lokalizacji. 4. System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykl. |
| <p>Odtwarzanie:</p> | <ol style="list-style-type: none"> 1. Odtwarzanie granularne: <ul style="list-style-type: none"> • Pojedynczych plików z kopii obrazu dysku • Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365 2. Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów) <ul style="list-style-type: none"> • Windows: 7+, • Windows Server: 2008 R2+, 3. Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. 4. Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a 5. Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|-----------------------|--|
| | <ol style="list-style-type: none"> 6. Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK) 7. Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL), Odtwarzanie zasobów plikowych z prawami dostępu. 8. Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows), 9. Odtwarzanie danych według harmonogramu 10. Przywracanie danych z określonego urządzenia/użytkownika 11. Przywracanie kopii z wybranego magazynu. Przywracanie danych Microsoft 365: <ul style="list-style-type: none"> • Do wskazanej , dowolnej lokalizacji na wybranym urządzeniu w formie pliku <ul style="list-style-type: none"> - pst - mbox • Do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego , w tym w innej organizacji) 12. System posiada możliwość nieodwracalnego kasowania danych. 13. Przywracanie repozytoriów GIT: <ul style="list-style-type: none"> • Przywracanie pomiędzy hostingami repozytoriów (GitGub/BitBucket) • Przywracanie między kontami |
| <p>Backup:</p> | <ol style="list-style-type: none"> 1. Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla: <ol style="list-style-type: none"> a) Systemów operacyjnych: <ol style="list-style-type: none"> vii. Alpine 3.10+, viii. Debian: 9+, ix. Ubuntu: 16.04+, x.Fedora: 29+, xi. centOS: 7+, xii. RHEL: 6+, xiii. openSUSE: 15+, xiv. SUSE Enterprise Linux(SLES): 12 SP2+, xv. macOS: 10.13+, xvi. Windows: 7, 8.1, 10(1607+), xvii. Windows Server: 2008 R2+, b) Środowisk wirtualnych: <ul style="list-style-type: none"> • Hyper-V, • VMware: 6.7+. c) Repozytoriów GIT: <ul style="list-style-type: none"> • GitHub • Bitbucket 2. Wykonywanie pełnych , różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|------------|--|
| | <ul style="list-style-type: none"> • Baza danych <ul style="list-style-type: none"> - Microsoft SQL - MySQL, - PostgreSQL, - Dowolnych innych przez podpięcie skryptów pre/post. <p>3. Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:</p> <ul style="list-style-type: none"> • 128 bit, • 192 bit, • 256 bit. <p>4. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:</p> <ul style="list-style-type: none"> • ZStandard • LZ4 <p>5. Oprogramowanie umożliwia zarządzanie poziomem kompresji 6. Wykonywanie kopii zapasowej otwartych plików(VSS) 7. System umożliwia uruchamianie skryptów przed i po backupie 8. System umożliwia uruchamianie skryptów po wykonaniu migawki VSS 9. System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów 10. Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT 11. Backup plikowy 12. Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe 13. Oprogramowanie umożliwia konsolidację wersji kopii zapasowych 14. Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego. 15. Oprogramowanie pozwala na backup zaszyfrowanych partycji.</p> |
| GIT | <p>1. Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych) 2. Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki)</p> |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|-------------------------|---|
| Licencjonowanie: | <ol style="list-style-type: none"> 1. Sposób licencjonowania opiera się na: <ul style="list-style-type: none"> • Ilości serwerów/endpointów- dla fizycznych urządzeń • Ilości fizycznych hostów - dla środowisk wirtualnych • Ilości repozytoriów - dla GIT. 2. Licencje powinny pozwalać na zabezpieczenie <ul style="list-style-type: none"> • 35 stacji roboczych w opcji dożywotniej • 4 serwery fizyczne w opcji dożywotniej 3. Wsparcie techniczne: <ul style="list-style-type: none"> • Świadczone w języku polskim, bezpośrednio przez główną siedzibę producenta • Zapewnia dostęp do aktualizacji oprogramowania • Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego • Okres wsparcia technicznego co najmniej 12 miesięcy |
|-------------------------|---|

Oprogramowanie do zarządzania infrastrukturą sieciową

| Nazwa | Opis przedmiotu zamówienia |
|---|--|
| Wymagania ogólne dla systemu zarządzania | <ol style="list-style-type: none"> 1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy 2. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej 3. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą 4. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników. 5. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompiowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit. 6. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną pracę wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych. 7. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|---|
| | <p>operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).</p> <ol style="list-style-type: none">8. Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).9. Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.10. Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-201911. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.12. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .13. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie przypisywania wybranych jednostek organizacyjnych, Jednostek lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty14. Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).15. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows16. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).17. Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej18. Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).19. Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.20. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieźdzeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU. |
|--|---|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|---|
| | <ol style="list-style-type: none"> 21. Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego. 22. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych 23. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej 24. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej. 25. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami. 26. Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień, predefiniowane atrybuty komputera. 27. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych 28. Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów. 29. Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty. 30. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika. |
| <p>Inwentaryzacja konfiguracji komputerów</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego 2. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu. 3. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej. 4. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| | <p>zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417</p> <ol style="list-style-type: none">5. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.6. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.7. Oprogramowanie musi umożliwiać analizę sprzętową:<ul style="list-style-type: none">• płyty głównej w zakresie model, producent, nr. seryjny,• CPU w zakresie nazwy, modelu, producenta, częstotliwości,• HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,• RAM w zakresie wielkości pamięci,• karty sieciowej w zakresie model, adres IP, adres MAC,• karty graficznej w zakresie model.8. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.9. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.10. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.11. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych12. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych13. Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora14. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera). |
|--|--|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|---|
| <p>Inwentaryzacja oprogramowania</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania. 2. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach 3. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.). 4. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem. 5. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach. 6. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu. 7. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office. 8. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji. 9. Oprogramowanie musi umożliwiać okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów. 10. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika. 11. Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji. |
| <p>Zarządzanie licencjami, audyt oprogramowania</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania 2. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe). 3. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade. 4. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji. 5. Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|---|
| <p>Zarządzanie zasobami oraz użytkownikami</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać klonowanie wybranych typów zasobów 2. Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami 3. Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu. 4. Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość. 5. Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów. 6. Oprogramowanie musi umożliwiać zdefiniowanie dodatkowych atrybutów dla wybranych relacji pomiędzy zasobami w zakresie zgodnym z atrybutami typów zasobów. 7. Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiający powiązania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem. 8. Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych. 9. Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów. 10. Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu. 11. Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV. 12. Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej |
| <p>Zdalny pulpit, zdalne zarządzanie komputerem</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpitu nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencje (ten sam proces systemowy). 2. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji |



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| | <p>zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.</p> <ol style="list-style-type: none">3. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).4. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.5. Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.6. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).7. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.8. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.9. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.10. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.11. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.12. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe13. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL14. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows15. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN16. Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połączenie konsoli ze wskazanym serwerem aplikacji.17. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem. |
|--|--|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|----------------------|--|
| Automatyzacja | <ol style="list-style-type: none">1. Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.2. Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.3. Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych4. Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.5. Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.6. Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.7. Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).8. Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).9. Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.10. Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.11. Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.12. Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk. |
|----------------------|--|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|---|--|
| | <p>13. Oprogramowanie musi umożliwiać optymalizację dystrybucji zadań oraz plików na komputery, pobierając brakujące fragmenty plików od agentów z tej samej podsieci (mechanizm peer-to-peer).</p> <p>14. Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:</p> <ul style="list-style-type: none"> - Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0) - Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0) - Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi - Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y. - Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego. <p>W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.</p> |
| <p>Backup danych użytkownika</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej. 2. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres). 3. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane. 4. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP. 5. Mechanizm archiwizacji danych musi być realizowany przez Agent systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów) 6. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji. 7. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| <p>Zarządzanie urządzeniami USB Storage</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny. 2. Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane. 3. Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage. 4. Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage 5. Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD |
| <p>Monitoring użytkowników</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jake stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony. 2. Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik. 3. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk). 4. Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach 5. Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego). 6. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk. 7. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione. 8. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności). 9. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer. 10. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania 11. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy. 12. Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć). 13. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP 14. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| | <p>zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej</p> <p>15. Oprogramowanie po zainstalowaniu musi przysyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.</p> <p>16. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urzędzeń drukujących (podział kosztu na mono/kolor).</p> |
| <p>ServiceDesk – Zarządzanie zgłoszeniami</p> | <ol style="list-style-type: none"> 1. Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności: <ul style="list-style-type: none"> • Zarządzanie problemem • Zarządzanie incydemem • Obsługa procesorów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy) • Zarządzenia umowami serwisowymi • Definicje poziomów SLA (reakcja, naprawa, reklamacja) 2. Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora. 3. Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika. 4. Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski). 5. Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień. 6. Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracownikami działu IT oraz przegląd awaryjności sprzętu. 7. Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP. 8. Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmu SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń. 9. Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu. 10. Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia. |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| | <ol style="list-style-type: none">11. Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.12. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.13. Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika14. Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.15. Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.16. Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników17. Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.18. Oprogramowanie musi umożliwiać tworzenie szablonów zadań.19. Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.20. Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu21. Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.22. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.23. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika24. Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.25. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika26. Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.27. Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.28. Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma |
|--|--|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| | <p>dostępu do PC (np. telefonicznie informuje, że zepsuł mu się komputer).</p> <ol style="list-style-type: none">29. Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).30. Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.31. Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.32. Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.33. Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.34. Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.35. Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.36. Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.37. Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).38. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).39. Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.40. Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc) |
|--|--|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| | <p>41. Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:</p> <ul style="list-style-type: none">• Zmiana statusu po przejściu zgłoszenia• Przejmowanie zadań po przejściu zgłoszenia przez opiekuna• Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia• Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika• Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika• Zamykanie zgłoszenia po upływie czasu reklamacji• Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów• Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza• Walidacja zamkniętych zadań w zamykanym zgłoszeniu• Systemowe potwierdzanie realizacji zgłoszenia• Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione <p>42. Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.</p> <p>43. Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.</p> <p>44. Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.</p> <p>45. Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).</p> <p>46. Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika</p> <p>47. Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia</p> <p>48. Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń</p> <p>49. Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem</p> <p>50. Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB</p> |
|--|--|

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|---|--|
| | <ol style="list-style-type: none"> 51. Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku) 52. Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia 53. Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia 54. Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja) 55. Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu 56. Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą 57. Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności 58. Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu |
| <p>ServiceDesk – Zarządzanie nieobecnościami</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa |
| <p>ServiceDesk – Zarządzanie wnioskami</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych). 2. Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika. 3. Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu. |
| <p>ServiceDesk – Zarządzanie uprawnieniami</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych 2. Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych 3. Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych) 4. Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|--|
| | <ol style="list-style-type: none"> 5. Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek 6. Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych 7. Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu) 8. Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku 9. Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika) 10. Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiarów danych dla poszczególnych osób 11. Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiarów danych 12. Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika |
| <p>ServiceDesk – Zarządzanie rezerwacjami</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie. 2. Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji. 3. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika. 4. Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem. 5. Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza. 6. Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników. |
| <p>Monitoring sieci LAN</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony 2. Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować o błędach takich jak brak papieru, zacięcie papieru. 3. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router. 4. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|--|---|
| | <p>poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.</p> <ol style="list-style-type: none"> 5. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP. 6. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia. 7. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING. 8. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email. |
| <p>Zarządzanie urządzeniami komputerowymi z systemem MacOS:</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać skanowanie komputerów z systemem MacOS w zakresie konfiguracji sprzętowej oraz zainstalowanego oprogramowania 2. Oprogramowanie musi umożliwiać, z listy stanowisk zarejestrowanych w konsoli systemu stanowisk, przejście pulpitu wybranego komputera |
| <p>System wewnętrznego komunikatora dla użytkowników</p> | <ol style="list-style-type: none"> 1. Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych. 2. Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostgreSQL 3. Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej 4. Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami 5. Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania. 6. Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia. 7. Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora). 8. Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej 9. Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej). 10. Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami. 11. Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych. 12. Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video). |

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | |
|----------------------------|--|
| | <ol style="list-style-type: none">13. Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami14. Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych. |
| Wymagania formalne: | <ol style="list-style-type: none">1. Dostarczone licencje na oprogramowanie muszą być bezterminowe.2. Dostarczone licencje na oprogramowanie muszą być dostarczone z 12 miesięcznym supportem producenta, liczonym od daty zakończenia wdrożenia.3. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta. |

Opracował:

BURMISTRZ
Piotr Łosos (1)

