**Część nr I.**

1. **Serwer - 2 szt.**

|  |  |
| --- | --- |
| Obudowa | * Typu RACK, wysokość nie więcej niż 2U; * Szyny umożliwiające wysunięcie serwera z szafy stelażowej; * Ramię porządkujące ułożenie przewodów z tyłu serwera; * Obudowa gotowa do zainstalowania 16 dysków twardych hot plug 2,5”; * Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; * Zainstalowane 4 szt. dyski SSD SATA 1,92 TB Read-Intensive; * Zainstalowane 5 szt. dysków SAS 10k 2,4TB ; * Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray |
| Płyta główna | * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera * Możliwość instalacji procesorów 38-rdzeniowych; * Zainstalowany modułu TPM 2.0 współpracujący z Windows Serwer 2022; * 6 złącz PCI Express generacji 4 w tym   + 3 fizyczne złącza o prędkości x16;   + 3 fizyczne złącza o prędkości x8; * 32 gniazda pamięci RAM; * Obsługa minimum 4TB pamięci RAM DDR4; * Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna * Wsparcie dla technologii:   + Memory Scrubbing   + SDDC   + ECC   + Memory Mirroring   + ADDDC; * Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) * Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; |
| Procesory | * Dwa procesory 8-rdzeniowy * Taktowanie 3,2GHz * architektura x86\_64   osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 154 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów w oferowanym serwerze). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/cpu2017.html |
| Pamięć RAM | * 256 GB pamięci RAM * DDR4 Registered * 3200Mhz |
| Kontrolery LAN | * Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 10Gbit SFP+, dostarczona wraz z wkładkami 10GB SFP+ MM, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; * Zainstalowana karta 4x1GB RJ-45, umieszczona w slocie PCI-E; |
| Kontrolery I/O | * Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug; * Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60, 2GB pamięci podręcznej cache oraz podtrzymaniem pamięci; |
| Porty | * Zintegrowana karta graficzna ze złączem VGA z tyłu; * 2 port USB 3.0 wewnętrzne; * 2 porty USB 3.0 na panelu przednim * 2 porty USB 3.0 dostępne z tyłu serwera; * Możliwość wyposażenia w port serial, możliwość wykorzystania portu serial do zarządzania serwerem; * Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; |
| Zasilanie, chłodzenie | * Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 900W; * Należy dostarczyć kable zasilające C13-C14 o długości min 2,5 metra. * Redundantne wentylatory hotplug; |
| Zarządzanie | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii   + informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:     - karty rozszerzeń zainstalowane w dowolnym slocie 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 zrządzającej serwera     - wentylatory     - bateria podtrzymująca ustawienia BIOS płyty główne     - zasilacze * system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia 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 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;   + Dostęp poprzez przeglądarkę Web, SSH;   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;   + Zarządzanie alarmami (zdarzenia poprzez SNMP)   + Możliwość przejęcia konsoli tekstowej   + Możliwość zarządzania przez 6 administratorów jednocześnie   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)   + Obsługa serwerów proxy (autentykacja)   + Obsługa VLAN   + Synchronizacja czasu poprzez protokół NTP   + Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej * Możliwość pobrania oprogramowanie zarządzającego i diagnostyczne wyprodukowanego przez producenta serwera umożliwiające 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); * Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; * Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * Serwer posiada 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. * BIOS UEFI w specyfikacji 2.7; |
| System Operacyjny | * Serwer ma być dostarczony wraz z systemem operacyjnym opisanym w pkt „Serwerowy system operacyjny + Cale dostępowe” |
| Gwarancja | * 5 lat gwarancji producenta serwera w trybie on-site z czasem reakcji najpóźniej w ciągu następnego dnia roboczego od zgłoszenia awarii. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); |
| Dokumentacja, inne | * 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 – wymaganie oświadczenie wykonawcy lub producenta; * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; * W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; * Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; * Zgodność z normami: CB, RoHS, WEEE, GS oraz CE; |

1. **Serwerowy system operacyjny+ CAL’e dostępowe**

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:
   1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   4. 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:
    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    2. 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:
    1. Login i hasło,
    2. Karty z certyfikatami (smartcard),
    3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez 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:
    1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    2. 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.

* 1. Zdalna dystrybucja oprogramowania na stacje robocze.
  2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
  3. 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.

* 1. Szyfrowanie plików i folderów.
  2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
  3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
  4. Serwis udostępniania stron WWW.
  5. Wsparcie dla protokołu IP w wersji 6 (IPv6),
  6. Wsparcie dla algorytmów Suite B (RFC 4869),
  7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
  8. 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:

Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

Obsługi 4-KB sektorów dysków

Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

1. 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.
2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
6. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim
7. Serwerowy system operacyjny w najnowszej wersji producenta oprogramowania dostępnej na rynku.
8. Dostawca wraz z systemem operacyjnym dostarczy 150 licencji User Cal w najnowszej wersji producenta oprogramowania dostępnej na rynku.
9. **Komputer stacjonarny z monitorem 41 szt.**

|  |  |
| --- | --- |
| **Podzespół** | **Minimalne parametry** |
| Procesor | Wydajność obliczeniowa: Procesor, który powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik 17500 punktów Passmark CPU Mark. |
| Płyta główna | * chipset dostosowany do oferowanego procesora lub równoważny * minimum 2 sloty pamięci lub więcej, obsługującej częstotliwość minimum 2999 MHz lub więcej * minimum 1 x PCI Express 3.0 x 16 * minimum 1 x PCI Express 3.0 x 4 (mechanicznie x16) * minimum 4x złącza SATA 6.0 Gb/s * minimum 1x M.2 dla dysku SSD o parametrach co najmniej PCIe 3.0 x4 |
| Pamięć operacyjna RAM | * minimum 16 GB DDR4 * minimum 1 wolny slot pamięci na płycie głównej, * minimalny rozmiar możliwego rozszerzenia obsługiwanej pamięci, zapewniony  i potwierdzony przez producenta komputera: 64 GB |
| Porty w tylnej części komputera | Komputer musi posiadać:   * minimum 2 x Display Port 1.4 z obsługą funkcji Multi-Stream, * minimum 4 x USB, w tym co najmniej 2x USB 3.2 Gen 1, 2x USB 2.0 * minimum 1 port sieciowy RJ-45, * osobne porty audio line-in i line-out   Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB oraz VIDEO nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
| Porty w przedniej części komputera | Komputer musi posiadać:   * minumum 5 x USB, w tym min. 2 porty USB 3.2 Gen 1, 3 porty USB 2.0 oraz 1 port USB 3.2 Gen 1 Typ C (ładownie do 15W) * port audio do podłączenia słuchawek z mikrofonem |
| Dysk twardy | * Minimum 512GB SSD z interfejsem M.2 NVMe, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego zainstalowanego na komputerze przez producenta, po awarii, do stanu fabrycznego (tryb OOBE dla systemu MS Windows) * Możliwość zamontowania w obudowie dwóch dysków 3,5 cala lub 2,5 cala. |
| Napęd optyczny | Nagrywarka DVD +/-RW |
| Karta dźwiękowa | Karta dźwiękowa zintegrowana z płytą główną, zgodna ze standardem High Definition 5.1 |
| Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Pełna obsługa funkcji i standardów DX12, OpenGL 4.5, OpenCL 2.1. Możliwość fabrycznego zainstalowania dodatkowej, dedykowanej karty graficznej z pamięcią własną min. 4 GB. Grafika zintegrowana w procesorze musi umożliwiać jednoczesną obsługę co najmniej dwóch monitorów. Na potrzeby obsługi większej liczby monitorów oferowany komputer musi umożliwiać jednoczesną obsługę monitorów podłączonych do grafiki zintegrowanej w procesorze oraz zainstalowanej osobnej karty graficznej (jeśli jest ona wymagana). |
| Karta sieciowa | Karta sieciowa 10/100/1000 Ethernet RJ-45, zintegrowana z płytą główną wspierająca obsługę technologii WoL oraz PXE. Zintegrowana karta sieciowa musi być wyposażona w diodę statusu informującą a aktywności połączenia oraz diodę informującą o prędkości połączenia. |
| BIOS | **BIOS UEFI w wersji 2.6 lub wyższej. Możliwość odczytania z BIOS informacji o:**   * modelu komputera, * numerze seryjnym, * AssetTag/IDTag * MAC Adres karty sieciowej, * wersja Biosu wraz z datą jego produkcji, * zainstalowanym procesorze, jego taktowaniu * ilości pamięci RAM wraz z taktowaniem i obłożeniem slotów   **Możliwość z poziomu BIOS:**   * wyłączenia selektywnego portów USB, minimum wyłączanie portów z przodu oraz wyłączanie portów z tyłu jako grup * wyłączenia selektywnego (pojedynczego) portów SATA, * zmiany pracy wentylatorów między trybem optymalizacji głośności lub temperatury, * ustawienia hasła: administratora, Power-On, HDD, * możliwość zbierania i przeglądania logów zdarzeń z informacją odnośnie godziny, daty i kodu błędu zdarzenia * ustawienie automatycznej aktualizacji BIOS z serwera producenta komputera |
| Klawiatura | Klawiatura USB w układzie polskim programisty (105 klawisze) z kablem o długości min. 1,8 m. |
| Mysz | Mysz optyczna USB z klawiszami oraz rolką (scroll) z kablem o długości min. 1,8 m. |
| Obudowa | * Typu Microtower przystosowana do pracy w pionie, z obsługą kart PCI Express; * Wbudowany głośnik do odtwarzania plików multimedialnych. * Suma wymiarów obudowy, nie może przekroczyć: 860 mm, najkrótszy z wymiarów nie większy niż: 180 mm * Obudowa jednostki centralnej beznarzędziowa, pozwalająca na demontaż komponentów i kart rozszerzeń (PCIe) oraz napędu optycznego i dysków twardych (co najmniej 3,5 cala) bez użycia narzędzi, z obiegiem powietrza tylko przód-tył - brak perforacji na bokach obudowy . * Głośność jednostki centralnej nie może przekraczać 18 dB, mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego. Wymagany raport badawczy, wystawiony przez niezależną, akredytowaną, co najmniej dla norm ISO 7779 i ISO 9296 jednostkę badawczą. |
| Zasilanie | Zasilacz o mocy nie mniejszej niż 280 W i nie większej niż 300 W, o sprawności 94% przy obciążeniu 50%. Roczny pobór mocy jednostki centralnej, nie większy, niż w specyfikacji energetycznej dla Energy Star w wersji 8.0. Zasilacz spełniający kryteria 80Plus PLATINUM według informacji podanej na stronie: <https://www.clearesult.com/80plus/> |
| Bezpieczeństwo i funkcje zarządzania | 1. Możliwość zastosowania mechanicznego zabezpieczenia przed kradzieżą komputera. 2. Zamek zatrzaskowy z kluczem, nie wystający poza obrys obudowy zabezpieczający przed niepowołanym dostępem do wnętrza obudowy. 3. Funkcjonalność TPM 2.0. 4. Certyfikowane oprogramowanie umożliwiające – bez względu na stan czy obecność systemu operacyjnego w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego - w ofercie należy podać nazwę i producenta oprogramowania. 5. System diagnostyczny działający bez udziału systemu operacyjnego, czy też jakichkolwiek dołączonych urządzeń na zewnątrz czy też wewnątrz komputera, umożliwiający otrzymanie informacji o:   - modelu, oznaczeniu i numerze seryjnym komputera, pojemności zainstalowanej pamięci RAM  **Oprogramowanie diagnostyczne musi umożliwiać:**   * wykonanie testu pamięci RAM, * wykonanie podstawowego testu prawidłowej pracy CPU * wykonanie testu dysku twardego.   System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera (Zaimplementowany w sprzętowym mikro kodzie płyty głównej) |
| Sterowniki  i oprogramowanie | Zapewnienie na dedykowanej stronie internetowej producenta dostępu do najnowszych sterowników i uaktualnień, realizowane poprzez podanie numeru seryjnego/modelu urządzenia, podać link strony www.  Oprogramowanie producenta komputera posiadające funkcje zarządzania sterownikami (wykrywanie i instalowanie aktualizacji).  Oprogramowanie umożliwiające – bez względu na stan czy obecność systemu operacyjnego oraz bez podłączania żadnych urządzeń czy nośników zewnętrznych - w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego. Usuwanie danych z dysku twardego musi odbywać się przy wykorzystaniu certyfikowanych algorytmów a wynikiem pracy oprogramowania musi być protokół zawierający dane kasowanego dysku oraz informacje o zastosowanym algorytmie kasowania. W ofercie należy podać nazwę i producenta oprogramowania. |
| Certyfikaty  i oświadczenia | 1. **Producent komputera musi posiadać ISO 9001 co najmniej w zakresie projektowania, produkcji i serwisu komputerów.** 2. **Producent komputera musi posiadać ISO 14001, co najmniej w zakresie projektowania i produkcji.** 3. **Oferowane komputery stacjonarne muszą posiadać europejską deklarację zgodności CE.** 4. **Certyfikat poprawnej współpracy z zaoferowanym systemem operacyjnym - do oferty dołączyć wydruk ze strony producenta oprogramowania systemowego.** 5. **Producent komputera/fabryka producenta musi posiadać normę ISO 50001.** 6. **Producent komputera musi posiadać normę ISO 27001.** 7. **Oferowane komputery stacjonarne muszą posiadać certyfikat TCO 9.0 – obecność modelu na stronie** [**https://tcocertified.com/product-finder/**](https://tcocertified.com/product-finder/) 8. **Oferowane komputery stacjonarne muszą posiadać certyfikat EPEAT dla standardu IEEE 1680.1 - 2018 – obecność modelu na stronie** [**https://www.epeat.net/?category=pcsdisplays**](https://www.epeat.net/?category=pcsdisplays)   **Powyższe oświadczenia i certyfikaty załączyć do ofety** |
| Zainstalowane oprogramowanie systemowe | Zainstalowany system operacyjny co najmniej Windows 10 Pro 64-bitowy w polskiej wersji językowej lub system równoważny wraz z nośnikiem instalacyjnym.  Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego.  *Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.*  System równoważny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,    2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim. 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 4. Wbudowany system pomocy w języku polskim. 5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. 8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. 9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4  i v6. 12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. 18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 22. Obsługa standardu NFC (near field communication). 23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 26. Mechanizmy logowania do domeny w oparciu o:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 27. Mechanizmy wieloelementowego uwierzytelniania. 28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. 30. Wsparcie dla algorytmów Suite B (RFC 4869). 31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. 32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. 35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 36. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 40. Udostępnianie modemu. 41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 43. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa  (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie  z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. 46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera,  z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. 49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. |
| Gwarancja – zgodnie z wymaganiami i kryteriami | Gwarancji jakości producenta:  Na okres co najmniej 24 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca,  Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego  W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony komputer zastępczy  Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta,  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela |
| **Monitor** | |
| Ekran | 23,8 cala o rozdzielczości natywnej minimum 1920x1080 pikseli, maksymalny rozmiar piksela 0.275 mm, matryca matowa, pokryta powłoką 3H, technologia matrycy IPS |
| Parametry obrazu | Odwzorowanie 16.7 miliona kolorów, kontrast typowy 1000:1,  jasność min. 250 cd/m2, czas reakcji matrycy max. 5ms, kąty widzenia pionowe/poziome minimum 178/178 stopni |
| Wejścia wideo i inne | 1x DP, 1x DVI-D, 1x D-SUB, wejście/wyjście audio |
| Obudowa i  regulacja monitora | Pochylenie ekranu w zakresie -5° / +22°(tzw. Tilt), zintegrowany zasilacz i głośniki stereo o mocy minimum 2W każdy, możliwość regulacji głośności z menu OSD monitora, złącze Kensington Lock, złącze montażu na ścianie w standardzie VESA |
| Funkcje zarządzana energią i parametrami wyświetlania obrazu | Technologia zapewniająca  zużycie energii przez monitor w trybie power save na poziomie 0.2W pozwalająca na redukcję ogólnego zużycia energii przez monitor (bez konieczności manualnego wyłączania monitora przez użytkownika), zgodność z normą Energy Star 8.0, zużycie energii przy ustawieniach EPA max. 14W |
| Menu monitora | Regulacja głośności  Regulacja jasności  Regulacja kontrastu  Regulacja koloru (sRGB, 5000K, 6500K, 7500K, Użytkownika (R,G,B)  Menu w języku polskim oraz angielskim. |
| Kable | kabel sygnałowy cyfrowy o długości minimum 1.8m, kabel zasilający o długości minimum 1,8m, kabel audio |
| Gwarancja | Gwarancja 24 miesięcy |
| Certyfikaty i normy, dokumentacja | -Klasa energetyczna D  -TCO 8.0  -Epeat Bronze  -TÜV Low Blue Light Certified  -TÜV Flicker Free Certified  -CE  -ISO9241-307(klasa I)  -RoHS, WEEE  -Instrukcja obsługi monitora |

1. **Komputer przenośny- laptop - 23 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Wymagane parametry techniczne** |  |
| Matryca | Komputer przenośny z ekranem  15” o rozdzielczości: FullHD (1920 x 1080) z podświetleniem LED, jasność matrycy min. 250 cd/m2 | |
| Wydajność | Procesor osiągający w teście PassMark Performance Test, co najmniej 10 000punktów w kategorii Average CPU Mark. Wynik dostępny na stronie: <https://www.cpubenchmark.net/cpu_list.php> na dzień 18.02.2022 r. | |
| Pamięć RAM | Min.  16 GB DDR4 możliwością rozbudowy do 32GB,  Jeden wolny  slot pamięci. | |
| Pamięć masowa | Min. 500 GB SSD | |
| Karta graficzna | Zintegrowana | |
| Multimedia | * karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, * wbudowane głośniki stereo, * mikrofon  wbudowany w obudowę matrycy, * klapka zasłaniająca kamerę | |
| Bateria i zasilanie | Bateria  4-cell o pojemności min. 47 WHR. Zasilacz min 45 W | |
| Waga i wymiary | Waga komputera z baterią nie większa niż 1.9 kg. | |
| Obudowa | Wykonana z trwałych materiałów. | |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). | |
| BIOS | * BIOS zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i samego urządzenia wskazującego (touchpad/mysz). oraz samego urządzenia wskazującego (touchpad/mysz). Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, numerze seryjnym i dacie produkcji komputera, wielkości, prędkości i sposobie obsadzenia zainstalowanej pamięci RAM w slotach, typie, ilości rdzeni, min. i maks. prędkości zainstalowanego procesora oraz wielkości pamięci cache L2 i L3 zainstalowanego procesora, zainstalowanym dysku twardym (a w szczególności o jego pojemności), MAC adresie wbudowanej w płytę główną karty sieciowej, kontrolerze video, kontrolerze audio, przekątnej i natywnej rozdzielczości zainstalowanej matrycy, zainstalowanej karcie sieci bezprzewodowej, poziomie naładowania baterii wraz z informacją o mocy podłączonego zasilacza. * Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB. * Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia haseł na poziomie użytkownika, administratora (oddzielne hasła) * możliwość włączenia/wyłączenia zintegrowanego kontrolera USB, kontrolera audio, kamery, mikrofonu, głośników. * Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania, które umożliwia min.: uruchamianie systemu z zainstalowanego HDD, uruchamianie systemu z urządzeń zewnętrznych typu HDD-USB, USB Pendrive, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, | |
| Bezpieczeństwo | * Układ szyfrowania TPM (Trusted Platform Module) lub analogiczny, * klawiatura odporna na zachlapanie lub zalanie * możliwość montażu na lince zabezpieczającej. | |
| Certyfikaty | * Deklaracja zgodności CE | |
| System operacyjny | 1. System operacyjny klasy PC musi spełniać poniższe wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. 2. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet oraz dodatkowo z możliwością wyboru instalowanych poprawek (możliwość scentralizowanego wyboru instalowanych poprawek dzięki dodatkowemu oprogramowaniu producenta). 3. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu. 4. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie w ofercie nazwy strony serwera WWW. 5. System musi umożliwiać pracę w domenie. 6. Wymagane jest aby dostarczona licencja systemu operacyjnego dopuszczała instalację systemu operacyjnego producenta, którego wsparcie dodatkowe wygasa nie wcześniej niż 1 października 2025 r. 7. Internetowa aktualizacja zapewniona w języku polskim. 8. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPv4 i IPv6. 9. Wbudowane narzędzie do szyfrowania dysków w oparciu o TPM komputera. 10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 11. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 12. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 13. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. 14. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 16. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 17. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. 18. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 19. Wbudowany system pomocy w języku polskim. 20. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 21. Zarządzanie stacją roboczą poprzez polityki rozumiane jako zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 22. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 23. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 24. Wsparcie dla logowania przy pomocy smartcard.  * Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. * Posiadanie narzędzi służących do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. * Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0, 4.0, 5.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. * Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. * Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. * Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. * Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. * Graficzne środowisko instalacji i konfiguracji. * Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. * Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. * Oprogramowanie dla tworzenia kopii zapasowych (backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. * Możliwość przywracania plików systemowych. * System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). * System musi posiadać możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). | |
| Wymagania pozostałe | Wbudowane porty i złącza:   1. 1xHDMI, 2. 1x RJ-45 (10/100/1000), 3. min.  3x USB 3.2 Gen 1 4. 1 x DisplayPort over USB-C 5. 1x Thunderbolt™ 4 over USB-C 6. czytnik kart multimedialnych w formacie co najmniej SD, 7. port audio combo (słuchawki oraz mikrofon), 8. gniazdo ładowania, 9. gniazdo linki zabezpieczającej, 10. zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11AC z modułem bluetooth. | |
| Warunki gwarancji | * gwarancja producenta na laptop) - min. 24 miesięcy | |

1. **Szkolenie z obsługi oprogramowania do wirtualizacji - 1 szt.**

Wykonawca zapewni szkolenie dla min 1 osoby w wymiarze 5 dniowym w trybie online umożliwiające instalowanie, zarządzanie i konfigurację dostarczonego systemu wirtualizacji.

Zakres szkolenia

Szkolenie koncentruje się na instalacji, konfiguracji oraz zarządzaniu dostarczonego systemu wirtualizacji. Szkolenie przygotowuje do administracji infrastrukturą wirtualną w organizacji o dowolnym rozmiarze.

Szkolenie to jest podstawą dla większości innych technologii wirtualizacji w data center definiowanym programowo.

Szkolenie przeznaczone jest dla Administratorów systemowych, inżynierów systemowych oraz innego  personelu, który  wykorzystuje rozwiązania bazujące na wirtualizacji

JĘZYK SZKOLENIA

* Szkolenie: polski
* Materiały: angielski

1. **Oprogramowanie wirtualizacyjne 1 szt.**

Wraz ze sprzętem należy dostarczyć oprogramowanie do wirtualizacji. Dostarczane oprogramowanie musi być w najnowszej wersji obecnie dostępnej na rynku.

Licencja dla 2 serwerów fizycznych posiadających 2 procesory ze wsparciem technicznym 9x5 z 4h-czasem zdalnej reakcji oraz gwarancją utrzymania aktualnej wersji przez okres min. 3 lat.

Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.

* Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
* Pojedynczy klaster może się skalować do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
* Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć

i wykorzystać procesory fizyczne wyposażone w 768 logicznych wątków oraz do 12TB pamięci fizycznej RAM.

* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-256 procesorowych.
* Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych

z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.

* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
* Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
* Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 11, SLES 12, SLES 15, RHEL 8, RHEL 7, RHEL 6, RHEL 5, RHEL 4, Solaris 11 ,Solaris 10, Debian, CentOS, FreeBSD, Asianux, Ubuntu 20, Ubuntu 18, Ubuntu 10, SCO OpenServer, SCO Unixware, Mac OS X, Amazon Linux 2, Oracle Linux.
* Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
* Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
* Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.
* Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
* Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
* Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
* Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
* Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.
* System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
* Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
* Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
* Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
* Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
* Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

1. **Switch 24T/48 - 2szt**

1. Typ i liczba portów:

48 portów 10/100/1000BaseT RJ-45 + uplink 4x10G SFP

3. Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:

* Gigabit Ethernet 1000Base-SX,
* Gigabit Ethernet 1000Base-LX/LH,
* 10Gigabit Ethernet 10GBase-SR,
* 10Gigabit Ethernet 10GBase-LR,
* 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

4. Urządzenie posiada funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi,

5. Zasilanie i chłodzenie:

* Urządzenie wyposażone jest w wbudowany zasilacz AC230V,

6. Parametry wydajnościowe:

* Przepustowość przełącznika (switching bandwidth):
  + 176 Gb/s (full duplex),
* Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3:
  + 77.38 Mpps,
* Pamięć DRAM – 512 MB
* Pamięć flash – 256 MB
* Wielkość bufora pakietów - 1.5 MB
* Obsługa:
* 256 aktywnych sieci VLAN
* 15000 adresów MAC
* 16 statycznych tras IPv4
* 16 statycznych tras IPv6
* 64 interfejsów SVI L3
* Obsługa MTU-L3 9198B
* Obsługa ramek Ethernet Jumbo 10240B
* 1024 grupy IGMP
* 6 połączeń zagregowanych typu „port channel”
* 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
* Ilość wpisów w listach kontroli dostępu Security ACL – 600
* ilość wpisów w listach kontroli dostępu QoS ACL – 600

7. Porty dostępowe przełącznika posiadają zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

8. Obsługa protokołu NTP

9. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping

10. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

* IEEE 802.1w Rapid Spanning Tree
* Per-VLAN Rapid Spanning Tree (PVRST+)
* IEEE 802.1s Multi-Instance Spanning Tree
* Obsługa 64 instancji protokołu STP

11. Obsługa protokołu LLDP i LLDP-MED

12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

13. Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad

14. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

15. Możliwość uruchomienia funkcji serwera DHCP

16. Mechanizmy związane z bezpieczeństwem sieci:

* Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
* Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
* Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
* Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
* Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication),
* Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
* Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
* Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
* Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
* Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP),
* Funkcja Private VLAN,

17. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:

* sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
* bezpieczna sekwencja uruchamiania,
* sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

18. Mechanizmy związane z zapewnieniem jakości usług w sieci:

* Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
* Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
* Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
* Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
* Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń,
* Kontrola sztormów dla ruchu broadcast/multicast/unicast,
* Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

19. Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6,

20. Przełącznik umożliwia lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących,

21. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),

22. Obsługa protokołu sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow,

22. Zarządzanie

* Port konsoli,
* Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika,
* Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
* Obsługa protokołów SNMPv3, SSHv2, https, syslog,
* Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia,
* Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;

23 Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU,

1. **Switch 24P/48 2 szt.**

1. Typ i liczba portów:

48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x10G SFP

2. Moc dostępna dla PoE:

370W (30W dla dowolnych 12 portów jednocześnie lub 15W dla dowolnych 24 portów jednocześnie),

3. Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:

* Gigabit Ethernet 1000Base-SX,
* Gigabit Ethernet 1000Base-LX/LH,
* 10Gigabit Ethernet 10GBase-SR,
* 10Gigabit Ethernet 10GBase-LR,
* 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

4. Urządzenie posiada funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi,

5. Zasilanie i chłodzenie:

* Urządzenie wyposażone jest w wbudowany zasilacz AC230V,
* Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia,

6. Parametry wydajnościowe:

* Przepustowość przełącznika (switching bandwidth):
  + 176 Gb/s (full duplex),
* Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3:
  + 77.38 Mpps,
* Pamięć DRAM – 512 MB
* Pamięć flash – 256 MB
* Wielkość bufora pakietów - 1.5 MB
* Obsługa:
* 256 aktywnych sieci VLAN
* 15000 adresów MAC
* 16 statycznych tras IPv4
* 16 statycznych tras IPv6
* 64 interfejsów SVI L3
* Obsługa MTU-L3 9198B
* Obsługa ramek Ethernet Jumbo 10240B
* 1024 grupy IGMP
* 6 połączeń zagregowanych typu „port channel”
* 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
* Ilość wpisów w listach kontroli dostępu Security ACL – 600
* ilość wpisów w listach kontroli dostępu QoS ACL – 600

7. Porty dostępowe przełącznika posiadają zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

8. Obsługa protokołu NTP

9. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping

10. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

* IEEE 802.1w Rapid Spanning Tree
* Per-VLAN Rapid Spanning Tree (PVRST+)
* IEEE 802.1s Multi-Instance Spanning Tree
* Obsługa 64 instancji protokołu STP

11. Obsługa protokołu LLDP i LLDP-MED

12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

13. Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad

14. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

15. Możliwość uruchomienia funkcji serwera DHCP

16. Mechanizmy związane z bezpieczeństwem sieci:

* Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
* Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
* Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
* Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
* Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication),
* Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
* Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
* Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
* Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
* Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP),
* Funkcja Private VLAN,

17. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:

* sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
* bezpieczna sekwencja uruchamiania,
* sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

18. Mechanizmy związane z zapewnieniem jakości usług w sieci:

* Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
* Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
* Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
* Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
* Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń,
* Kontrola sztormów dla ruchu broadcast/multicast/unicast,
* Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

19. Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6,

20. Przełącznik umożliwia lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących,

21. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),

22. Obsługa protokołu sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow,

22. Zarządzanie

* Port konsoli,
* Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika,
* Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
* Obsługa protokołów SNMPv3, SSHv2, https, syslog,
* Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia,
* Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;

23 Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU,

1. **NAS + oprogramowanie backupowe - 1 szt.**

|  |  |
| --- | --- |
| **Nazwa elementu, parametru lub cechy** | **Opis wymagań minimalnych** |
| Procesor | Min 4-rdzeniowy procesor 1,7 GHz |
| Pamięć systemowa | 8 GB pamięci SODIMM DDR3 (1 x 8 GB) |
| Maksymalna ilość pamięci | 8 GB |
| Obudowa | RACK 1U |
| Pamięć Flash | 512 MB (ochrona przed podwójnym rozruchem systemu operacyjnego) |
| Wnęka na dyski | 4 x 3,5-calowy SATA 6 Gb/s, 3 Gb/s |
| Zgodność z dyskami | 3,5-calowe kieszenie: 3,5-calowe dyski twarde SATA 2,5-calowe dyski twarde SATA 2,5-calowe dyski półprzewodnikowe SATA |
| Możliwość wymiany podczas pracy | tak |
| Obsługa akceleracji pamięci podręcznej SSD | tak |
| Port Gigabit Ethernet (RJ45) | 2 |
| Port 10 Gigabit Ethernet | 1 x 10GbE SFP+ |
| Port USB 3.2 Gen 1 | 4 |
| Przyciski | Zasilanie, Reset |
| Ostrzeżenie systemowe | brzęczyk |
| Gniazdo zabezpieczające Kensington | Tak |
| Sumaryczna pojemność dyskowa | 4 x12000 GB (48 TB) |
| Parametry zainstalowanych dysków | Interfejs: Serial ATA III  Pojemność HDD: 12000GB  Szybkość HDD: 7200 RPM  Rozmiar HDD: 3.5"  Rozmiar bufora dysku pamięci: 256MB  MTBF (Średni okres międzyawaryjny): 2000000 h  Szybkość transmisji interfejsu HDD: 6GB/s  Kompatybilność: dyski powinny znajdować się na liście kompatybilności serwera NAS z bieżącego zamówienia.  Gwarancja: 60 miesięcy |
| Gwarancja na serwera NAS | 24 miesiące |

**Oprogramowanie backupowe**

1. Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji

a) Microsoft Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012

b) Vmware vSphere min. w wersjach v4.1-7.0

c) Nutanix AHV 5.10 (LTS)

d) Maszyny fizyczne: Windows Server 2019, 2016, 2012R2, 2012, 2008R2

2. Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V

3. Oprogramowanie musi pozwalać na wdrożenie w środowiskach

a) na serwerze sprzętowym, obsługiwane systemy operacyjne w ramach: Windows Server 2008 R2 – 2019 (x64), Windows 7 – 10 Professional (x64), Ubuntu 16.04 – 18.04 Server (x64), Red Hat Enterprise Linux 7.4 – 7.6 (x64), SUSE Linux Enterprise Server 12 SP1-SP3 (x64), CentOS 7.6

b) jako maszyna wirtualna Vmware

c) jako maszyna wirtualna Amazon

d) na serwerze NAS najbardziej popularnych producentów

4. Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS

5. Oprogramowanie nie może wymagać instalacji jakiegokolwiek agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania

6. Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji (np. Frameworków czy baz danych)

**II Licencjonowanie**

1. Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności

2. W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 3 lat wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania

4. W ramach dostawy wymagane jest dostarczenie licencji na ochronę min 4 gniazd procesorów w hostach środowisk wirtualizacyjnych

5. Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska

**III Ochrona danych**

1. Oprogramowanie musi posiadać funkcje backupu i replikacji:
2. Backup maszyn wirtualnych Vmware
3. Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
4. Backup maszyn wirtualnych Hyper-V
5. Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
6. Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
7. Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
8. Oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
9. Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych

Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem

1. Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
2. Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
3. Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach.

**IV Optymalizacja wykorzystania miejsca na dane**

1. Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
2. Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
3. Kompresja backupu, w tym konfigurowalny stopień kompresji
4. Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne

V **Spójność danych**

1. Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
2. Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
3. Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
4. Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
5. Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
6. Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
7. Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji

**VI Przywracanie danych**

1. Oprogramowanie musi posiadać poniższe funkcje:
2. Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
3. Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku wirtualizacji(bez wcześniejszego przywracania maszyny wirtualnej)
4. Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
5. Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):

Microsoft Exchange

MS Active Directory

MS SQL

1. Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.

**VII Wydajność**

1. Oprogramowanie do backupu musi pozwalać na:
2. Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
3. Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
4. Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
5. Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
6. Wsparcie dla urządzeń oferujących dodatkową deduplikację danych

**VIII Zarządzanie**

1. Oprogramowanie musi pozwalać na następujące formy zarządzania:
2. Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
3. Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
4. Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
5. Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
6. Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
7. Oprogramowanie musi umożliwiać integrację z Active Directory
8. Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach
9. **Zasilacz awaryjny UPS – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa elementu, parametru lub cechy** | **Opis wymagań** |
| Moc pozorna | 2200 VA |
| Moc rzeczywista | 2200 W |
| Topologia (klasyfikacja IEC 62040-3) | Line-interactive z AVR |
| Współczynnik mocy | 1 |
| Czas przełączenia na baterię | <4 ms |
| Liczba, typ gniazd wyjściowych | 8 x IEC C13 (2 grupy po 2 gniazda IEC C13 gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza ), 1 x IEC C19 16A |
| Typ gniazda wejściowego | IEC C20 16A |
| Czas podtrzymania dla 100% obciążenia dla pf=1 | 3 min |
| Czas podtrzymania przy 50% obciążenia dla pf=1 | 10 min |
| Dodatkowe baterie | Możliwość dodania do 4 dodatkowych modułow baterii w celu wydłużenia czasu podtrzymania do 95 minut dla 100% obciążenia przy pf=1 |
| Napięcie znamionowe | 200/208/220/230/240/250 V |
| Tolerancja napięci prostownika | 160 V – 294 V (regulacja programowa 150-294 V) |
| Częstotliwość znamionowa | 50/60 Hz autodetekcja |
| Tolerancja częstotliwości | 47– 70 Hz |
| Kształt napięcia | Sinusoidalny |
| Napięcie znamionowe wyjściowe | 200/208/220230/240 V do wyboru przez użytkownika |
| Zakres zmian napięcia | +6/-10% napięcia nominalnego |
| Częstotliwość wyjściowa | 50/60 Hz |
| Współczynnik szczytu | 3:1 |
| Baterie wymieniane przez użytkownika "na gorąco" | Tak |
| Ochrona przed przeładowaniem | Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm) |
| Ochrona przed głębokim rozładowaniem | Tak |
| Okresowy automatyczny test baterii | Tak |
| System zarządzania pracą baterii | **System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii.** W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. |
| Możliwość uruchomienia bez napięcia w sieci | Tak |
| Baterie wewnętrzne o pojemności nie mniejszej niż | 7Ah 12V, minimum 6 szt. |
| Czas ładowania baterii do poziomu 90% | < 3 godz. do 90% pojemności użytkowej |
| Interfejs komunikacyjny | •  USB |
| • RS232 DB-9 żeński (HID) |
| • styki przekaźnikowe |
| • miniport wyłącznik ON/OFF |
| • SNMP/Ethernet |
| Panel sterowania z wyświetlaczem LCD | • Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny,napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh). |
| • Poziomy rząd przycisków sterowania |
| • Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony) |
| • Sygnalizator akustyczny |
| Sygnały akustyczne | • Awaria |
| • Niski stan naładowania baterii |
| • Przeciążenie |
| • Serwis |
| Przyciski sterujące i wskaźniki diodowe LED | • Przycisk Escape (anulowanie) |
| • Przyciski funkcyjne (przewijanie w górę i w dół) |
| • Przycisk Enter (potwierdzający) |
| • Przycisk ON/OFF załączenia i wyłączenia |
| • LED trybu zasilania z siec i(kolor zielony) |
| • LED trybu baterii (kolor żółty) |
| • LED usterki (kolor czerwony) |
| Kolor | Czarny RAL 9023 / RAL 9005 |
| Typ obudowy | Uniwersalna Tower/Rack 2U |
| Wyposażenie standardowe | UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa |
| 1 x kabel szeregowy RS-232, |
| 1 x kabel komunikacyjny USB |
| 1 x CD Oprogramowanie Solution Pack |
| 2 x kable wyjściowe IEC 10A |
| 2 x uchwyty kablowe |
| 1 x zestaw szyn montażowych 19’ |
| 1x kabel wejściowy |
| 1x karta sieciowa SNMP/Ethernet |
| Dane techniczne karty SNMP | Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/ |
| Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). Blokowanie konta: Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni. |
| Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI |
| Kamptybilność: SNMP v1/v3 i IP v4/v6 |
| Interfejs: HTML5 |
| Adresowanie IP: DHCP/BootP/Manualne |
| Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256 |
| Dostępny port USB (microUSB - port serwisowy) |
| Certyfikaty: CA, UL 2900-1, 2900-2-2 |
| Dołączone oprogramowanie | Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych:  - Windows:  7 / 8 / 2008 / Vista / 2003 / XP - Microsoft SCVMM 2012 - Linux: Debian GNU Linux: Lenny,  SUSE/Novell: SLES 11, OpenSUSE 11.2,  Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12  Ubuntu: 10.04 - VMWare: vCenter / ESXi 5.1  - Citrix XEN 6.0 |
| Zgodność ze standardem Energy Star | Tak |
| Maksymalna szerokość | 438 mm |
| Maksymalna wysokość | 86 mm |
| Maksymalna głębokość | 603 mm |
| Maksymalny ciężar | 29 kg |
| Poziom hałasu w odl. 1m | do 45 dBA dla pracy normalnej |
| Znaki bezpieczeństwa | CE, TUV, CB Report, IEC/EN 62040-1-1, IEC/EN 62040-2 |
| Gwarancja producenta | 24 mc dla elektroniki |
| Możliwość montażu ręcznego bypassu serwisowego | Tak |

1. **Wykonanie bezpiecznej i odpowiednio zabezpieczonej strony www Urzędu Gminy - dostosowanie strony www do najnowszych standardów WCAG 2.1, oraz Szkolenia dla pracowników Urzędu z obsługi BIP - 1 szt.**

**Minimalne wymagania techniczno-funkcjonalne nowej strony internetowej:**

* Charakteryzuje się zminimalizowanym czasem załadowania.
* Strona internetowa jest prosta i intuicyjna w użytkowaniu, nowoczesna i przejrzysta.
* Wyświetla się prawidłowo w następujących przeglądarkach WWW: Edge, Firefox, Opera, Google Chrome.
* Strona internetowa zostanie zoptymalizowana do rozdzielczości poziomej 1024 pikseli z wyłączonym skalowaniem w przypadku gdy użytkownik używa większej rozdzielczości.
* Strona internetowa jest zrealizowana zgodnie z wymaganiami WCAG 2.1 (Web Content Accessibility Guidelines) dla systemów teleinformatycznych w zakresie dostępności dla osób niepełnosprawnych, zgodnie z zapisami Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
* Strona internetowa jest responsywna - dostosowuje się do rozdzielczości urządzenia na jakim jest oglądana (telefon komórkowy, tablet, PC).
* Strona internetowa zostanie wykonana z wykorzystaniem technologii PWA (Progressive Web Application) tzn. strona internetowa będzie posiadała możliwość „zainstalowania” na uprzędzeniu mobilnym, a jej zawartość zapisywana jest w pamięci urządzenia. Dzięki zapisanym danym, ponowne wejście na stronę PWA może odbyć się również w trybie offline.
* Kodowanie polskich znaków w serwisie internetowym odbywa się wg standardu UTF-8.
* Strona po wdrożeniu posiada kod zgodny z rekomendacją W3C HTML 5.
* Strona internetowa wyposażona jest w mechanizm automatycznej archiwizacji dokumentów z określonym czasem publikacji i możliwości korzystania z archiwum. Administrator ma możliwość swobodnej decyzji dotyczącej przedłużenia czasu publikacji, automatycznej archiwizacji lub usunięcia artykułów.
* W trakcie czytania wybranego artykułu na stronie, użytkownik ma możliwość zmiany wielkości tekstu (pomniejszenie/powiększenie czcionki); wydruku; ściągnięcia pliku do pobrania; wysyłki treści e-mailem w formie funkcji „Wyślij znajomym" - wysyłanie do znajomego bezpośrednio ze stron WWW, rekomendacji z informacją o istnieniu danej podstrony.
* Serwis internetowy zawiera wyszukiwarkę umożliwiającą Użytkownikowi przeszukiwanie serwisu zarówno proste, jak i zaawansowane - z uwzględnieniem kryteriów.
* Strona internetowa umożliwia odtwarzania zdjęć oraz elementów multimedialnych (audio, video).
* Strona posiada mechanizm umożliwiający wyświetlenie informacji o czasowej niedostępności serwisu z powodów technicznych.
* Strona zawiera mechanizm automatycznej archiwizacji dokumentów z określonym czasem publikacji i możliwości korzystania z archiwum. Administrator strony ma możliwość decyzji dotyczącej przedłużenia czasu publikacji, automatycznej archiwizacji lub usunięcia artykułów.
* Mapa serwisu tworzona jest automatycznie.

**Specyfikacja techniczno-funkcjonalna Narzędzia administracyjnego CMS (Content Management System – System Zarządzania Treścią):**

* System CMS i dokumentacja (instrukcja obsługi) wykonane są w języku polskim.
* Przy tworzeniu artykułów występuje możliwość pokazania skrótu aktualności wpisywanego ręcznie lub tworzonego automatycznie z treści wiadomości.
* CMS realizuje swoje zadania przy użyciu przyjaznego i łatwego w obsłudze interfejsu.
* Posiada opcję ustawienia dowolnego zdjęcia w artykule w położeniu pionowym lub poziomym.
* Posiada możliwość dołączenia elementów dynamicznych do wszystkich tekstów.
* Posiada możliwość zintegrowania z zewnętrznymi serwisami np. Facebook.
* Importuje oraz generuje kanał RSS.
* Umożliwia dowolne ustawianie kolejności elementów w strukturze serwisu i w treści artykułu.
* Posiada mechanizm umożliwiający załadowanie plików graficznych (zdjęć) w dużej rozdzielczości (do pobrania) wraz z systemem ich prezentacji na stronie artykułowej.
* CMS jest przystosowany do obsługiwania nieograniczonej ilości nazwanych użytkowników, czyli odrębnych kont w systemie.
* Narzędzia administracyjne (w tym CMS) umożliwiają dalszą rozbudowę serwisu po zakończeniu prac nad wdrożeniem.
* Nawigacja z poziomu administratora opiera się na strukturze drzewiastej.
* Zmiany na stronie są widoczne natychmiast po zapisaniu.
* Posiada funkcję udostępnienia podglądu zdjęć oraz edytowanych stron przed ich opublikowaniem.
* Moduł edycyjny umożliwia:
  + - dodawanie, zmianę lub usuwanie elementów treści strony;
    - wstawienie i edycję tabel (m.in.: edycja komórek, wierszy, kolumn i ich właściwości);
    - dodawanie plików i obiektów z prezentacjami;
    - dodawanie oraz prezentacja zdjęć i plików multimedialnych;
    - dodawanie treści z serwisu Youtube;
    - możliwość druku z poziomu edytowanego tekstu;
    - pogrubienie, pochylenie i podkreślenie tekstu;
    - wyśrodkowanie, wyjustowanie, dociąganie do lewej lub prawej strony;
    - wklejenie tekstu z plików tekstowych, Worda, Excela, OpenOffice;
    - wklejenie tekstu bez formatowania;
    - skorzystanie z dostępnych stylów zastosowanych w serwisie;
    - stworzenie listy numerowanej i punktowanej;
    - cofnięcie ostatnich operacji;
    - wstawienie, edycję i usunięcie hiperłącza, linków wewnątrz dokumentu (anchor);
    - wstawienie grafiki, możliwość ustawienia jej względem tekstu (oblanie itd.);
    - wstawienie linii poziomej;
    - wstawienie tekstu w formie indeksu górnego lub dolnego;
    - edycji w źródle dokumentu;
    - zmianę wielkości obszaru roboczego (na dowolny oraz do pełnego ekranu);
    - podłączenie galerii zdjęć;
    - wstawianie niestandardowych znaków np. §;
    - wyszukiwanie tekstu, z opcją zamiany na inny;
    - włączanie/wyłączanie wyświetlania niedrukowalnych elementów np. paragrafów, twardych spacji;
    - wstawianie tzw. „twardej spacji” - stosowanej w edytorze Word/OpenOffice;
    - usunięcie formatowania z zaznaczonej części lub całości dokumentu;
    - wstawianie czystego kodu HTML;
    - System CMS umożliwia administratorom tworzenie kont użytkowników oraz nadawanie im uprawnień do poziomu konkretnych działów.
* Posiada opcję samodzielnego tworzenia działów i struktury serwisu oraz zmiany kolejności wyświetlania działów w menu. Istnieje możliwość ukrycia działu tak, żeby istniał w strukturze, ale nie był widoczny na stronie.
* Opcja ustawienia kolejności wyświetlania tekstów na stronie.
* System automatycznie zmniejsza przesyłane zdjęcia do określonego rozmiaru wraz  z utworzeniem miniatury. Posiada opcję stworzenia samej miniatury bez naruszania oryginalnego zdjęcia.
* Umożliwia wklejanie odnośnika do filmu YouTube jako miniatura do aktualności.
* Umożliwia zmianę rozdzielczości i orientacji obrazu przy edycji pliku z poziomu CMS.
* Posiada mechanizm automatycznej zmiany ścieżek do opublikowanych plików po zmodyfikowaniu nazwy lub położenia katalogu lub pliku.
* Posiada mechanizm automatycznego nadawania wartości atrybutu title dla odnośników - następuje automatyczne uzupełnienie informacji o rodzaju linku (link zewnętrzny, link wewnętrzny, odnośnik do pliku) i jego atrybutów (akcji, która się wykona po kliknięciu lub wielkość pliku).
* System udostępnia dane statystyczne związane z oglądalnością serwisu.
* Publikuje treści o zadanej wcześniej dacie.
* Umożliwia określenie daty zakończenia publikacji zakładek.
* Umożliwia włączenie automatycznego, cyklicznego powiadamiania administratorów o konieczności aktualizacji wybranych zakładek menu.
* Posiada funkcję automatycznego ukrywania zakładek w przypadku wygaśnięcia daty obowiązywania treści.
* Umożliwia duplikowania gałęzi menu w inne miejsce struktury.
* Umożliwia duplikowanie aktualności.
* Umożliwia przywrócenie treści aktualności lub informacji z rejestru zmian CMS.
* Zapewnienia maksymalne bezpieczeństwo przed niepowołanym dostępem z zewnątrz.
* Posiada możliwość dodania jako plik do pobrania dokumentów w formatach:.gif, jpg, png, tif, bmp, zip, tar, tgz, gz, rar, exe, mov, mpg, mpeg, webp, webm, avi, asf, mp3, mp2, rm, wav, vob, qt, vid, ac3, wma, wmv, doc, xls, ppt, pdf, docx, xlsx, pptx, rtf, txt, swf, odt, ods.
* Ma możliwość uruchomienia szybkiego przełączenia między różnymi wersjami kolorystycznymi serwisu np. czarno-białą, świąteczną, itp.;
* Posiada możliwość samodzielnej wymiany banerów.
* Posiada możliwość administrowania serwisem zawierającym treści w dowolnym języku obcym.

W zakres wdrożenia wchodzi również dostawa licencji i wdrożenie oprogramowania - urzędowego publikatora teleinformatycznego stworzonego w celu powszechnego udostępniania informacji publicznej w postaci ujednoliconego systemu stron w sieci teleinformatycznej, zwanego dalej „Biuletynem Informacji Publicznej”, zgodnie z przepisami ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2018 poz.1330 z póź. zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz.U. Nr 10, poz. 68) oraz ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2019 poz. 848).

**Funkcjonalność BIP**

* 1. Oprogramowanie ma mieć architekturę trójwarstwową, złożoną z:
     + elementu klienckiego, o serwera aplikacji, o serwera bazy danych, zarządzającego SQL-ową bazą danych.
  2. Serwis powinien wyświetlać się prawidłowo w następujących przeglądarkach WWW: o Edge,
     + Firefox, o Opera, o Google Chrome.

1. Serwis ma być zoptymalizowany do minimalnej rozdzielczości poziomej 1024 pikseli.
2. Kodowanie polskich znaków wg standardu UTF-8.
3. Strona spełnia wymaganie zgodności ze standardami: W3C, HTML 5.00, CSS 3, WCAG 2.1.
4. W trakcie czytania wybranego artykułu na stronie, użytkownik ma mieć możliwość:
   * + zmiany wielkości tekstu (pomniejszenie/powiększenie czcionki), o zmiany kontrastu, o wydruku,
     + wysyłki treści e-mailem w formie funkcji „Wyślij znajomym" - wysyłanie do znajomego bezpośrednio ze stron WWW, rekomendacji z informacją o istnieniu danej podstrony,
     + przeglądania rejestru zmian wprowadzonych informacji.
5. Strona BIP posiada:
   * + wyszukiwarkę umożliwiającą użytkownikowi przeszukiwanie serwisu zarówno proste, jak i zaawansowane - z uwzględnieniem kryteriów typu: data graniczna, ograniczenie do tytułów i/lub treści, ograniczenie do konkretnej gałęzi w menu,
     + mechanizm umożliwiający wyświetlenie zaprojektowanej przez wykonawcę informacji o czasowej niedostępności serwisu z powodów technicznych,
     + mechanizm automatycznej archiwizacji dokumentów z określonym czasem publikacji i możliwości korzystania z archiwum. Administrator ma mieć możliwość decyzji (oraz jej zmiany) dotyczącej przedłużenia czasu publikacji, automatycznej archiwizacji lub usunięcia artykułów,
     + możliwość przeglądania zmian we wszystkich podstronach z okresu ustalonego w panelu administracyjnym,
     + mapę serwisu tworzoną automatycznie,
     + rozwiązanie generujące statystyki łącznej ilości odwiedzin oraz poszczególnych podstron i artykułów, o strukturę wielopoziomową bez ograniczeń,
     + modułu SIOS (System Informacji o Środowisku), o modułu Karty informacyjne Usług – procedura załatwiania sprawy.

**Narzędzia administracyjne, w tym CMS (Content Management System – System Zarządzania Treścią)**

* 1. Aplikacja CMS zawiera pełną instrukcję obsługi panelu CMS w języku polskim.
  2. Aplikacja ma realizować swoje zadania przy użyciu przyjaznego i łatwego w obsłudze interfejsu i ma umożliwiać:
     + dołączanie elementów dynamicznych do wszystkich tekstów,
     + dowolne ustawianie kolejności elementów w strukturze serwisu i w treści artykułu, o automatyzację najczęściej powtarzanych czynności administracyjnych, o podgląd edytowanych stron przed ich opublikowaniem, o definiowanie rozszerzeń plików używanych w CMS, o wysyłanie plików o wielkości do 256MB, o publikację artykułu lub informacji w maksymalnie 10 kliknięciach od zalogowania, o tworzenie działów i struktury serwisu oraz zmiany kolejności wyświetlania działów w menu,
     + ukrycie działu tak, żeby istniał w strukturze, ale nie był widoczny na stronie,
     + ustawienie kolejności wyświetlania tekstów na stronie, o dokonanie wyboru typu artykułu – aktualność lub informacja, o powiązania ze sobą dowolnej ilości aktualności, o konwersję informacji na aktualność,
     + rejestrowanie statystyk wyszukiwarki BIP (wyrażenia i frazy wpisywane do wyszukiwania), o publikowanie treści o zdefiniowanej dacie, o jednoczesne przesyłanie wielu plików na serwer, o automatyczne usunięcie plików nieużywanych w BIP, o wyłączenia archiwizowania określonych artykułów, o samodzielne rejestrowanie się użytkowników w BIP, o ograniczenia dostępu do artykułu dla osób zalogowanych, o filtrowanie plików dostępnych podczas edycji treści według kryterium czasu utworzenia.
  3. Nawigacja z poziomu administratora powinna opierać się na strukturze drzewiastej.
  4. BIP wykorzystuje narzędzie do analizy statystyk serwera i oglądalności serwisu.
  5. Zmiany na stronie muszą być widoczne natychmiast po zapisaniu.
  6. Aplikacja automatycznie generuje listę redaktorów BIP.
  7. Moduł edycyjny ma umożliwiać:
     + dodawanie, zmianę lub usuwanie elementów treści strony,
     + wstawienie i edycję tabel (m.in.: edycja komórek, wierszy, kolumn i ich właściwości), o dodawanie plików i obiektów z prezentacjami, o dodawanie oraz prezentację zdjęć i plików multimedialnych, o możliwość druku z poziomu edytowanego tekstu, o pogrubienie, pochylenie i podkreślenie tekstu, o wyśrodkowanie, wyjustowanie, dociągniecie do lewej i prawej strony, o wklejenie tekstu z plików tekstowych aplikacji typu Word, Excel, OpenOffice, o wklejenie tekstu bez formatowania,
     + skorzystanie z dostępnych stylów zastosowanych w serwisie, o stworzenie listy numerowanej i punktowanej,
     + cofnięcie ostatnich operacji,
     + wstawienie, edycję i usunięcie hiperłącza, linków wewnątrz dokumentu (anchor), o wstawienie grafiki, możliwość ustawienia jej względem tekstu, o wstawienie linii poziomej,
     + wstawienie tekstu w formie indeksu górnego lub dolnego, o edycję w źródle dokumentu,
     + zmianę wielkości obszaru roboczego do pełnego ekranu, o wstawianie niestandardowych znaków np. §, o wyszukiwanie tekstu, z opcją zamiany na inny,
     + włączanie/wyłączanie wyświetlania niedrukowalnych elementów np. paragrafów, twardych spacji,
     + wstawianie tzw. „twardej spacji” - stosowanej w edytorze Word/OpenOffice, o usunięcie formatowania z zaznaczonej części lub całości dokumentu, o wstawianie czystego kodu HTML.
  8. Aplikacja umożliwia administratorom dodawanie nieograniczonej ilości nazwanych użytkowników, czyli odrębnych kont w aplikacji oraz nadawania im uprawnień:
     + do konkretnych modułów,
     + do pozycji w menu, z rozdzieleniem na edycję, publikację wraz z dziedziczeniem z pozycji nadrzędnej w strukturze menu.
  9. Aplikacja posiada możliwość sortowania artykułów wg następujących kryteriów:
     + data udostępniania dokumentu, o data wytworzenia dokumentu, o tytuł artykułu.

**Bezpieczeństwo**

Wykonawca zapewni bezpieczeństwo funkcjonowania strony podmiotowej - logowanie, ochrona danych, hierarchizacja dostępu, hierarchia uprawnień, szyfrowanie, ochrona danych osobowych. Wykonawca zapewni niezbędne zabezpieczenia przed nieuprawnionymi zmianami na stronie, przekierowaniami, atakami oraz zabezpieczy dane znajdujące się na serwerze przed możliwością wykradzenia. Zapewni możliwość bezpiecznej autoryzacji osób uprawnionych, logujących się do niego przy pomocy przeglądarki internetowej. Wymagania szczegółowe:

* 1. Dostęp poprzez szyfrowane połączenie SSL.
  2. Zapewnienie obsługi certyfikatów dostępnych dla przeglądarek.
  3. Rejestracja wszystkich prób uwierzytelniania.
  4. Strona będzie posiadała rejestr modyfikacji dowolnej podstrony od momentu jej wprowadzenia. Rejestr winien gromadzić i przechowywać co najmniej następujące informacje:
     + dokładna data z godziną modyfikacji,
     + wszystkie operacje przeprowadzone na elementach strony, o dane użytkownika, który dokonał zmian, o krótki opis operacji (np. publikowanie, modyfikacja, cofanie publikacji, itp.), o pełną treść modyfikowanego dokumentu.

Strona będzie zabezpieczona w sposób, który zwiększa jej odporność na różne rodzaje ataków, ze szczególnym uwzględnieniem ataków typu SQL Injections, Dos, Cross-Site Scripting (XSS) i Cross Site ReguestForgery (CSRF).

**Wykonawca przeprowadzi szkolenia z wdrożonego oprogramowania dla pracowników Urzędu Miasta. Szkolenia odbędą się stacjonarnie lub zdalnie. Informację o wyznaczonym terminie szkoleń wykonawca powinien podać min 3 dni wcześniej**

1. **Oprogramowanie zabezpieczające- antywirus – 140 szt.**

|  |  |  |
| --- | --- | --- |
| Bezpieczeństwo i oprogramowanie dodatkowe – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:  • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,  • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,  • stosowanie kwarantanny,  • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)  • skanowanie urządzeń USB natychmiast po podłączeniu,  • automatyczne odłączanie zainfekowanej końcówki od sieci,  • skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.  • Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.  • Musi posiadać moduł ochrony IDS/IPS  • Musi posiadać mechanizm wykrywania skanowania portów  • Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów  • Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3. Mac OS X, Mac OS 10  4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:   * Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę * Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.   Zarządzanie użytkownikiem   * Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email * Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika * Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi * Musi posiadać możliwość eksportu danych użytkownika   Zarządzanie urządzeniem   * Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO * Musi umożliwiać import listy urządzeń z pliku CSV * Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych * Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta * Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał * Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres * Musi zawierać podgląd aktualnie zainstalowanych aplikacji * Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, * Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł * Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres   Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:   1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:   - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari   1. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 2. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 3. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:   - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a)           przegląd wybranych danych na podstawie konfigurowalnych widgetów  b)           zablokowania możliwości zmiany konfiguracji widgetów  c)            zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d)           tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e)           eksport wszystkich skanów podatności do pliku CSV |
| Wymagania dodatkowe | Dołączone oprogramowanie w momencie dostawy musi być zainstalowane na wszystkich dostarczonych laptopach (8szt) oraz stacjach roboczych (15szt) | |
| Długość licencji | Min. 24 miesiące | |

1. **Pakiet-Oprogramowanie biurowe - 64 szt.**

|  |  |
| --- | --- |
| Pakiet biurowy | Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.  2. Wymagania odnośnie interfejsu użytkownika:  a. Pełna polska wersja językowa interfejsu użytkownika.  b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.  3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:  a. Posiada kompletny i publicznie dostępny opis formatu.  b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2  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.  c. Pozwala zapisywać dokumenty w formacie XML.  4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego.  5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).  6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.  7. Pakiet zintegrowanych aplikacji biurowych musi zawierać:  a. Edytor tekstów.  b. Arkusz kalkulacyjny.  c. Narzędzie do przygotowywania i prowadzenia prezentacji.  d. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).  8. Edytor tekstów musi umożliwiać:  a. 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.  b. Wstawianie oraz formatowanie tabel.  c. Wstawianie oraz formatowanie obiektów graficznych.  d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).  e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.  f. Automatyczne tworzenie spisów treści.  g. Formatowanie nagłówków i stopek stron.  h. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.  i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  j. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.  k. Wydruk dokumentów.  l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.  m. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016 i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.  n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.  p. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.  9. Arkusz kalkulacyjny musi umożliwiać:  a. Tworzenie raportów tabelarycznych.  b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.  c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.  d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML).  e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.  f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.  g. Wyszukiwanie i zamianę danych.  h. Wykonywanie analiz danych przy użyciu formatowania warunkowego.  i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.  j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  k. Formatowanie czasu, daty i wartości finansowych z polskim formatem.  l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.  m. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013, 2016 i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.  n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  a. Przygotowywanie prezentacji multimedialnych, które będą:  b. Prezentowanie przy użyciu projektora multimedialnego.  c. Drukowanie w formacie umożliwiającym robienie notatek.  d. Zapisanie jako prezentacja tylko do odczytu.  e. Nagrywanie narracji i dołączanie jej do prezentacji.  f. Opatrywanie slajdów notatkami dla prezentera.  g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.  h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.  i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.  j. Możliwość tworzenia animacji obiektów i całych slajdów.  k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.  l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016 i 2019.  11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.  b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.  c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.  d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.  e. Automatyczne grupowanie wiadomości poczty o tym samym tytule.  f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.  g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.  h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.  i. Zarządzanie kalendarzem.  j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.  k. Przeglądanie kalendarza innych użytkowników.  l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.  m. Zarządzanie listą zadań.  n. Zlecanie zadań innym użytkownikom.  o. Zarządzanie listą kontaktów.  p. Udostępnianie listy kontaktów innym użytkownikom.  q. Przeglądanie listy kontaktów innych użytkowników.  r. Możliwość przesyłania kontaktów innym użytkowników.  s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http. |

1. **Szkolenia dla urzędników w zakresie cyberbezpieczeństwa** **- 1 szt.**

W ramach zadania wykonawca przeprowadzi szkolenia w zakresie cyberbezpieczeństwa dla pracowników Urzędu Miasta Sanoka. Szkolenia powinny odbywać się w 2 grupach nie większych niż 15 osób i trwać nie dłużej niż 2h/grupa. Szkolenia przeprowadzone będą w siedzibie zamawiającego– budynek Urzędu Miasta. Wykonawca przekaże harmonogram szkolenia nie później niż 7 dni przed rozpoczęciem szkolenia.

Program szkolenia:

1. System cyberbezpieczeństwa

• Podstawowe narzędzia cyberbezpieczeństwa

• Z czego powinien składać się skuteczny system cyberbezpieczeństwa i jak go zbudować.

1. Podejrzane urządzenia elektroniczne

• Przykłady zagrożeń laptopy, pendrive, smartfony

• Jak się przed tym chronić?

1. Ransomware

• Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje

• Jak się chronić i na co zwracać uwagę aby nie paść ofiarą cyberprzestępców

1. Phishing jak działa i na co zwracać uwagę

• Phishing – czym jest, jak działa?

• Przykłady zagrożeń związanych z Phishingem

1. Typowe zagrożenia występujące w internecie

• Prezentacja z wykorzystanie symulatora zagrożeń internetowych

Wykonawca podczas szkoleń zapewni dostęp do nowoczesnej platformy w formie strony www dostępnej w standardzie WCAG 2.1 – symulator zagrożeń internetowych. Szkolenia obędą się z wykorzystaniem dostarczonych komputerów przenośnych- laptop opisanych w pkt 4 niniejszego dokumentu. Symulator musi być narzędziem umożliwiającym użytkownikowi w bezpieczny sposób sprawdzenie oraz poznanie typowych zagrożeń czyhających na użytkowników w Internecie. Korzystanie z symulatora musi być całkowicie bezpieczne dla użytkownika końcowego (żadne z wpisywanych danych nie mogą być zapisywane i archiwizowane). W symulatorze konieczne jest zaimplementowanie min. 8 scenariuszy (zagrożeń) popularnych przestępstw internetowych, z którymi użytkownicy mogą się spotkać podczas codziennego korzystania z Internetu. Pierwsze cztery dotyczące tzw. Phishing’u w różnych odsłonach, ((Phishing Clone, Phishing Spear, Phishing Spear Chat, Phishing Whaling) następny dotyczy oszustwa typu Pharming, dwa kolejne mają przedstawiać zasadę działania zagrożenia typu Malware, (Malware Post, Malware Email,) natomiast ostatni dotyczący certyfikatów SSL (Certificate Fraud Chat) . Wykonawca zobowiązany jest przekazać zamawiającemu dostępy do platformy na min 30 dni od daty szkolenia, wraz z instrukcją obsługi.

Wymagania szczegółowe dla platformy Symulującej zagrożenia internetowe:

1. Moduł podstron (fałszywych witryn) – moduł ten będzie umożliwiał tworzenie różnego rodzaju fałszywych witryn nakłaniających użytkowników do pobierania zainfekowanych załączników, podawania danych wrażliwych i/lub dokonywania płatności internetowych.
2. Moduł czatu – w module tym zaimplementowany zostanie czat z botami, namawiającymi do zakupów różnych produktów powodując wyłudzenie danych osobowych, numerów kart kredytowych itp. Itd. W module tym zostaną zaimplementowane opracowane scenariusze
3. Moduł e-mail – w module tym użytkownik będzie miał do przeglądnięcia kilka wiadomości e-mail przesłanych z różnych źródeł, wiadomości te będą zawierały linki bądź załączniki po kliknięciu których, zostanie uruchomiona akcja symulująca zachowanie się malware, np. blokada komputera (przeglądarki) na jakiś określony czas. Po kliknięciu załącznika „zainfekowanego” na ekranie powinna pojawić się informacja na temat, że twój komputer został zainfekowany, wykradliśmy twoje dane osobowe itd. Itp. W tym module należy również pokazać działanie tzw. szyfrującego wirusa, który po kliknięciu w załącznik szyfruje wszystkie pliki tekstowe, w tym przypadku symulator powinien pokazać przykład
4. Moduł edukacyjny – moduł zawierający szczegółowe informacje na temat występujących cyberprzestępstw. W szczególności powinien się skupić na phishingu, pharmingu oraz malware.

* Moduł ten powinien zawierać informacje na temat występowania oraz identyfikacji danego zagrożenia, sposobów zapobiegania, oraz informacji na temat, co użytkownik powinien w pierwszej kolejności zrobić, gdy zostanie już oszukany – czyli gdzie się zgłosić najpierw, jakie dane zabezpieczyć, zmienić hasła, czy zablokować karty płatnicze.
* Materiały edukacyjne powinny być przedstawione w formie plików PDF przedstawiających, na co zwrócić szczególną uwagę podczas korzystania z portali społecznościowych, różnego rodzaju czatów, różnego rodzaju serwisów internetowych oraz odbierania wiadomości e-mail.
* Moduł edukacyjny powinien być ściśle zintegrowany z pozostałymi modułami tj. Po przejściu każdego z opracowanych i zaimplementowanych w symulatorze scenariuszy powinna pojawić się informacja o tym jak i dlaczego użytkownik dał się oszukać i jakie to może mieć konsekwencje w późniejszym czasie.

1. Moduł postów społecznościowych, zawierający możliwe ataki phishingowe lub pharmingowe, w module postów społecznościowych będą znajdować się zarówno „rzeczywiste” posty nie stanowiące zagrożenia jaki i posty z potencjalnym zagrożeniem.

**Część nr II.**

* 1. **Modernizacja wewnętrznej sieci Urzędu Miasta**

**Modernizacja sieci wewnętrznej - zakres skrócony:**

1. Wykonanie projektu sieci Ethernet kat 6a SFTP - 192 punkty logiczne oraz sieci elektrycznej.

2. Wykonanie okablowania (trasy kablowe, ułożenie okablowania, punkty logiczne) sieci Ethernet kat. 6A SFTP oraz dostarczenie i montaż szaf teleinformatycznych, gniazdek elektrycznych i modernizacja sieci elektrycznej.

3. 3 punkty przełączania (szafy rackowe 18U) wyposażone w patch panele 48portowe, oraz optyczne 12 FO.

4. Wykonanie okablowania światłowodowego pomiędzy punktami przełączania 12j,

5. Zakończenie nowo wykonanego okablowania strukturalnego miedzianego i optycznego w patchpanelach w szafach teleinformatycznych.

6. Pomiary statyczne i dynamiczne połączeń miedzianych i optycznych,

7. Demontaż starego okablowania miedzianego,

8. Prace budowlane odtworzeniowe,

9. Dokumentacja powykonawcza wraz z certyfikacją.

10. Serwis: Zamawiający wymaga gotowości do świadczenia szybkich usług serwisowych w okresie gwarancji na poziomie min.

Czas reakcji - 4 godz.

Czas usunięcia awarii - 9 godz.

11. Okres trwania gwarancji na wykonanie usługi- min 12 mc

**Modernizacja sieci wewnętrznej - zakres szczegółowy:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Wykonawca powinien zapoznać się ze strukturą pomieszczeń Zamawiającego przed złożeniem oferty w celu oszacowania kosztów realizacji prac związanych z wykonaniem instalacji sieci komputerowej wraz z siecią elektryczną. W tym celu Zamawiający udostępni pomieszczenia urzędu w godzinach otwarcia, tj. poniedziałek - piątek 10.00-14.00, po wcześniejszym jego powiadomieniu przez Wykonawcę, na numer tel.: 13 46 328 00, 13 46 528 11, 13 46 32819  Instalacja sieci komputerowej odbędzie się w terminie i w sposób uzgodniony z Zamawiającym, zapewniając ciągłość funkcjonowania urzędu.  Instalacja musi być wykonana zgodnie z wytycznymi producenta okablowania strukturalnego oraz wytycznymi norm referencyjnych w szczególności:   * EN 50174-1:2009/A1:2011 Information Technology - Cabling system installation- Part 1. Specification and quality assurance, wraz z jej polskim odpowiednikiem: PN-EN 50174-1:2010/A1:2011 Technika informatyczna - Instalacja okablowania - Część 1 - Specyfikacja i zapewnienie jakości (lub równoważne); * EN 50174-2:2009/AB2013 Information Technology - Cabling system installation - Part 2. Installation planning and practices internal to buildings, wraz z jej polskim odpowiednikiem: PN-EN 50174-2:2010/A1:2011 Technika informatyczna - Instalacja okablowania -Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków (lub równoważne); * EN 50174-3:2013 Information Technology - Cabling system installation - Part 3. – Industrial premises, wraz z jej polskim odpowiednikiem: PN-EN 50174-3:2014-02E Technika informatyczna - Instalacja okablowania - Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków (lub równoważne); * EN 50310:2010 Application of equipotential bonding and earthling at premises with information technology equipment, wraz z jej polskim odpowiednikiem: PN-EN 50310:2012 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym co winno zostać potwierdzone w dokumentacji powykonawczej (lub równoważne);   Zamawiający w odniesieniu do powyższych norm dopuszcza rozwiązania równoważne zgodne z powyższym opisem.  Planowane miejsce instalacji punktów logicznych, tras kablowych, rozmieszczenie urządzeń sieci LAN odbędzie się w lokalizacjach uzgodnionych z Zamawiającym. (Ostateczna lokalizacja punktów logicznych powinna być ustalona i potwierdzona na piśmie z Zamawiającym przed rozpoczęciem prac projektowych i instalacyjnych).   * **Zakres prac:** * 96 punktów logicznych i sieci elektryczna zlokalizowane będzie w dwóch segmentach. Pierwszy i drugi segment piętro najwyższe * 48 punktów logicznych i sieci elektryczna zlokalizowane będzie w trzecim segmencie. piętro środkowe, * 48 punktów logicznych i sieci elektryczna zlokalizowane będzie w trzecim segmencie. czwarty segment - parter. * Wykonanie okablowania (trasy kablowe poziome i pionowe, ułożenie okablowania, punkty logiczne, lokalizacja gniazd) sieci Ethernet kat. 6A SFTP * Instalacja nowych koryt tras kablowych (poziomych i pionowych) zapewniających min. 50% zapasu wolnej przestrzeni dla kabli sieci Ethernet dla koryt zbiorczych, oraz min 25% wolnej przestrzeni dla kabli Ethernet dla koryt punktów końcowych. Dodatkowo każdo z koryt powinno posiadać wydzielony wewnętrzny tor dla poprowadzenia przewodów zasilania prądem przemiennym 50/60 Hz o napięciu 240 V oraz przewodu uziemienia. * W miarę możliwości technicznych i ekonomicznych , przełożenie przewodów zasilania elektrycznego z obecnych tras do nowo położonych wraz z instalacją gniazd PE (punkt zasilania elektrycznego sprzętu komputerowego z sieci dedykowanej) * Wykonać trzy punkty pośrednie przełączania wyposażone w szafy wiszące rackowe 18U, wyposażone w patch panele adekwatne do przyłączonych do nich segmentów, oraz w patchpanele optyczne 12xSC SIMPLEX. * Wykonanie okablowania światłowodowego pomiędzy punktami przełączani, ułożyć kabel światłowodowy wewnętrzny zgodny z normą VDE: U-DQ(ZN)BH 12 włóknowy, w skrzyniach umieścić odpowiednio 30m zapasu. * Zakończenie nowo wykonanego okablowania strukturalnego miedzianego i optycznego w patchpanelach w szafach teleinformatycznych. * Pomiary statyczne i dynamiczne połączeń miedzianych i optycznych, * Demontaż starego okablowania miedzianego, * Dokumentacja powykonawcza wraz z certyfikatem * Roboty poinstalacyjne: uzupełnienie ubytków tynków powstałych w trakcie rozbudowy sieci, wykonanie powstałych miejscowych uzupełnień malarskich farbą emulsyjną, prace porządkowe, wywóz gruzu i zdemontowanych, złomowych elementów poinstalacyjnych. * Wszystkie elementy pasywne składające się na okablowanie strukturalne muszą być oznaczone nazwą lub znakiem firmowym, tego samego producenta okablowania i pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania certyfikatu gwarancyjnego w/w producenta na okres 25lat; * Producent okablowania strukturalnego musi legitymować się ważnym certyfikatem systemu zarządzania od minimum 10 lat co gwarantuje Użytkownikowi właściwą obsługę procesów sprzedażowych i utrzymaniowych. * Środowisko, w którym będzie instalowany osprzęt kablowy jest środowiskiem biurowym i zostało ono sklasyfikowane, jako łagodne wg. skali M1I1C1E1 * Konfiguracja oraz rozmieszczenie gniazd końcowych odbędzie się w lokalizacjach uzgodnionych z Zamawiającym * Okablowanie ma być zrealizowane w oparciu o moduł gniazda RJ45 Kat. 6A SFTP * Zgodnie z wymaganiami norm każdy 4 – parowy kabel ma być trwale zakończony na ekranowanym module RJ45 umieszczonym w gnieździe od strony użytkownika oraz na panelu krosowym w szafie; * Panele krosowe 24 portowe w Głównych Punktach Dystrybucyjnych mają mieć wysokość 1U. Panele muszą być wyposażone w półkę kablową oraz posiadać dedykowane miejsce na przypięcie uziemienia. * Moduł przyłączeniowy powinien charakteryzować się następującymi cechami: * Konstrukcja zapewniająca możliwość jednoczesnego zaterminowania wszystkich żył (konstrukcja bez narzędziowa, z możliwością zastosowania dedykowanego narzędzia terminującego), styki pokryte warstwą złota, szczęki IDC pokryte warstwą srebra. * Front modułu musi być wyposażony w elastyczną, demontowaną przesłonę przeciw kurzową. Zastosowane przesłony powinny być dostępne w kilku różnych kolorach co pozwoli na wprowadzenie systemu identyfikacji gniazd wraz z kodowaniem na kablach przyłączeniowych. * Kontakt szczęk IDC z żyłą przewodu powinna być ustawiona pod kątem 45 stopni co wydatnie poprawia parametry transmisyjne toru. Moduł musi posiadać wyraźne oznaczenie producenta, serii, kategorii, oraz schematu rozszycia w sekwencji T568A oraz T568B. * W celu zagwarantowania jak najwyższych marginesów pracy i zapasów parametrów transmisyjnych nie dopuszcza się rozwiązań złożonych z elementów różnych producentów, (tj. kabla, gniazd, kabli krosowych, itp.). Aby zagwarantować rzeczywiste i powtarzalne parametry toruoraz potwierdzić zgodność proponowanego rozwiązania z najnowszymi edycjami obowiązujących standardów międzynarodowych i niezależność od dostawcy komponentów wymagane jest na wezwanie Zamawiającego (tylko oferta wygrywająca) przedstawienie odpowiednich certyfikatów wydanych przez niezależne laboratoria uwzględniające najnowszą metodę kwalifikacji komponentów sieciowych. * **Kable i przewody:**   Okablowanie poziome ma być prowadzone nieekranowanym kablem typu: SFTP paśmie przenoszenia przewyższającym obowiązujące normy, min. 500 MHz w osłonie LSZH (powłoka wytwarzająca mało dymu, bezhalogenowa) o średnicy żyły: 23AWG (0,574mm), maksymalnej średnicy zewnętrznej 6,1 mm, koloru niebieskiego.  Dostarczone patchcordy powinny być wykonane techniką zaciskania, pochodzić od tego samego producenta co całość okablowania strukturalnego i oznaczone logo producenta na wtykach. W celu osiągnięcia najlepszych parametrów nie dopuszcza się rozwiązań zalewanych. W celu ułatwienia zarządzania połączeniami warstwy fizycznej patchcordy powinny mieć możliwość wykonania w różnych wariantach kolorystycznych.  Tabela. Wymagane właściwości dla kabla miedzianego segmentu okablowania poziomego   |  |  | | --- | --- | | Kategoria zgodnie z ISO11801 ed.2.2. (lub równoważny) | 6a | | Klasyfikacja ogniowa | LSZH - IEC 60332-1; IEC 60754-2; IEC 61034 | | Ekranowanie | SFTP | | Klasa separacji | B | | Zakres częstotliwości [MHz] | 500 | | ø żył [AWG] | 23 | | Max ø zewnętrzna kabla mm] | 5,4 | | Min promień gięcia instalacja [mm] | 45 | | Min promień gięcia użytkowanie [mm] | 25 | | Max Waga [kg/km] | 35,7 | | NVP | 68 |   Tabela. Wymagane właściwości dla kabli przyłączeniowych   |  |  | | --- | --- | | Kategoria zgodnie z ISO11801 ed.2.2. (lub równoważny) | 6a | | Klasyfikacja ogniowa | LSZH - IEC 60332-1; IEC 60754-2; IEC 61034 | | Ekranowanie | SFTP |   Wymagane właściwości dla kabli optycznych:  Kabel jednomodowy 12j o konstrukcji jednotubowej,  Włókna jednomodowe typu G.657.A2  Powłoka trudnopalna B2ca przebadana i zgodna z rozporządzeniem CPR 305/2011  ZW-NOTKtsdD / U-DQ(ZN)BH - SM 12J 9/125 LSOH  WŁAŚCIWOŚCI FIZYCZNE  Średnica zewnętrzna 6,1 mm\* (tolerancja średnicy zewnętrznej kabla +/- 5%)  Waga 12 włókien: 45 kg  Maks. siła ciągnienia (statyczna) 1000 N  Rodzaj włókna G.657.A2  Maks. siła ciągnienia (dynamiczna) 2000 N  Odporność na zgniatanie (max.) 200 N/cm  Min. promień zgięcia podczas instalacji R = 50 mm  Odporność na wodę odporny na wzdłużną penetrację wody poprzez zastosowanie pęczniejącego materiału  Euroklasa CPR B2ca  BUDOWA  Elementy wytrzymałościowe otulina z włókien szklanych  Powłoka zewnętrzna LSOH - bezhalogenowa, odporna na UV, grubość 1,3mm, kolor żółty, nadruk informacyjny biały, licznik długości co 1m  Kolor włókien 1. Czerwony, 2. Zielony, 3. Żółty, 4. Niebieski, 5. Biały, 6. Fioletowy, 7. Pomarańczowy, 8. Czarny  TEMPERATURA  Składowania od -40°C do +70°C  Instalacji od -5°C do +60°C  Pracy od -40°C do +70°C   * **Elementy terminowania kabli:**   **Moduły przyłączeniowe** stanowią kluczowy element zapewniający poprawna transmisje danych. Moduł przyłączeniowy musi charakteryzować się następującymi własnościami:   * Sposób terminacji żył kabla w module musi być wykonany za pomocą technologii IDC, jako powszechnie uznaną za najbardziej niezawodną metodę terminacyjną. * Moduł musi posiadać uchylną osłonę przeciwkurzową w różnych kolorach tak aby uzyskać również funkcjonalność kodowania kolorem za pomocą jednego elementu. * Metoda terminacji kabla instalacyjnego w module musi gwarantować niezależność jakości uzyskanego kontaktu od stanu i jakości samego narzędzia terminującego * Moduł musi zapewniać ochronę strefy kontaktu poprzez przytwierdzenie kabla instalacyjnego do obudowy modułu.   Pozostałe wymagane właściwości modułu przedstawia tabela poniżej:  Tabela. Wymagane właściwości dla modułu przyłączeniowego   |  |  | | --- | --- | | Kategoria zgodnie z ISO11801 ed.2.2.(lub równoważny) | 6A | | Zakres ø żył kabla [AWG] | 26-22 | | Min ilość cykli połączeniowych | 750 | | Schematy rozszycia kabla | TIA 568A/B | | Trwałość IDC | >200 cykli łączeniowych | | Niepalność obudowy | UL94V-0 |   Zgodnie z wymaganiami norm każdy 4-parowy kabel ma być trwale zakończony na nieekranowanym module RJ-45 umieszczonym w gnieździe od strony użytkownika oraz na panelu krosowym w szafie.  Wyspecyfikowane powyżej kable miedziane należy właściwie wprowadzić i zaterminować w panelach krosowych. Panele muszą charakteryzować się szeregiem własności funkcjonalnych oraz użytkowych pozwalających na sprawne, wygodne i oszczędne użytkowanie systemu okablowania przez cały okres jego eksploatacji:  **Panel krosowy**:   * Panel musi zajmować 1U miejsca w szafie 19” * Zagęszczenie portów musi zapewniać obsługę min 24 portów w 1U * Panel musi mieć budowę modularną pozwalającą uzyskać elastyczność w jego wyposażaniu o skalowalności od 1 do 24 portów * Panel krosowy musi posiadać zintegrowaną półkę kablową umożliwiającą przytwierdzenie wprowadzonego kabla za pomocą opaski zaciskowej lub taśmy typu rzep, co zabezpiecza moduły przyłączeniowe przed nieprężeniami pochodzącymi od kabla. * System w skład którego wchodzi panel musi umożliwiać kodowanie kolorem co poprawia walory administracyjne rozwiązania * Dodatkowo każdy port musi być ponumerowany   **Gniazda Abonenckie** (PL) zaprojektowano w standardzie instalacyjnym wybranego systemu okablowania.  Płyta czołowa PEL dla adapterów miedzianych musi być płytą prostą co ułatwia użytkowanie gniazd.  Gniazda muszą być wyposażone w widoczne pola opisowe zabezpieczone mechanicznie przed przypadkowym uszkodzeniem/zdarciem.  Moduł RJ-45 typu keystone powinien charakteryzować się następującymi cechami:  Konstrukcja zapewniająca możliwość jednoczesnego zaterminowania wszystkich żył (konstrukcja beznarzędziowa, narzędzie terminujące), separator par na wejściu do modułu krosowniczego, styki pokryte warstwą złota, szczęki IDC pokryte warstwą srebra, kontakt szczęk IDC z żyłą przewodu powinna być ustawiona pod kątem 45 stopni, wykonane z materiałów niepalnych UL 94V-0, wyraźne oznaczenie producenta, serii, kategorii oraz schematu rozszycia w sekwencji T568A/B. W celu ułatwienia zarządzania połączeniami – moduły powinny mieć możliwość identyfikacji za pomocą wymiennych, kolorowych przesłon przeciwkurczowych.  Moduły krosownicze muszą posiadać potwierdzenie zgodności z normami okablowania strukturalnego, uwzględniające również metodę klasyfikacji komponentów De-embedded oraz Re-embedded.   * Gniazda (moduły) RJ-45 oraz panele krosujące powinny spełniać wymogi urządzeń instalowanych wewnątrz budynków w pomieszczeniach nie narażonych na wpływ zewnętrznych warunków atmosferycznych. * Osprzęt sieci strukturalnej (gniazda, panele montażowe, moduły RJ-45, sznury połączeniowe i przyłączeniowe) powinny być kompatybilne z innymi systemami okablowania strukturalnego. * **Wymagania dotyczące systemu okablowania strukturalnego – punkt logiczny (PL):** * Minimalne wymagania wydajności elementów / systemu okablowania strukturalnego: * System okablowania ma posiadać wydajność klasy E potwierdzoną przez niezależne laboratorium. * Kategoria 6a SFTP oraz RJ-45 jako interfejs końcowy dla połączeń na skrętce miedzianej 4 parowej. * Kable wyprowadzone (od tyłu) z panela rozdzielczego (patchpanel) do istniejącej szafy teleinformatycznej 42 U. * Do każdego punktu dostępowego należy doprowadzić oddzielny kabel 4 parowy. * Na odcinku od punktu dystrybucyjnego do gniazdka nie można wykonywać łączy. * Maksymalna długość kabla instalacyjnego (tzw. łącza stałego) nie może przekroczyć 90 m. * Kable należy układać wzdłuż ścian budynku, w przestrzeni sufitu podwieszanego lub korytach kablowych. * PL – punkt logiczny = 1 gniazdo z interfejsem RJ-45. * Klasa zestawionych kanałów transmisyjnych oraz łącz stałych od patchpanela do PL – min. E z gwarantowanym pasmem przenoszenia min. 500 MHz. * **Testowanie**   Pomiary należy wykonać zgodnie z wymaganiami producenta okablowania strukturalnego oraz norm referencyjnych w szczególności:   * EN 50346:2002/A1:2007/A2:2009 Information Technology - Cabling system installation - Testing of installed cabling, wraz z jej polskim odpowiednikiem: PN-EN 50346:2004/A1:202009/A2:2010 Technika informatyczna - Instalacja okablowania - Badanie zainstalowanego okablowania (lub równoważne); * EN 61935-1:2009 Specification for the testing of balanced and coaxial information technology cabling - Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards, wraz z jej polskim odpowiednikiem: PN-EN 61935-1:2010E Wymagania dotyczące sprawdzania symetrycznych i współosiowych kablowych linii telekomunikacyjnych -- Część 1: Okablowanie z symetrycznych kabli telekomunikacyjnych zgodne z serią norm EN 50173 (lub równoważne); * ISO/IEC 14763-3:2006/A1:2009 Information technology –Implementation and operation of customer premises cabling – Part 3: Testing of optical fibre cabling, wraz z jej polskim odpowiednikiem: PN-ISO/IEC 14763-3:2009/A1:2010P Technika informatyczna - Implementacja i obsługa okablowania w zabudowaniach użytkowych - Część 3: Testowanie okablowania światłowodowego (lub równoważne);   Zamawiający w odniesieniu do powyższych norm dopuszcza rozwiązania równoważne zgodne z poniższym opisem.  Mierniki użyte w procesie pomiarowym muszą uzyskać aprobatę producenta systemu okablowania   * Testowanie statyczne powinno zostać wykonane testerem, który umożliwia sprawdzenie następujących cech poszczególnych odcinków kabli miedzianych: * zamiana przewodów w parze, * zamiana przewodów pomiędzy parami, * zwarcie w parze, * zwarcie między parami, * zwarcie do folii ekranującej, * brak połączenia. * Pomiary dynamiczne powinny zostać wykonane dla następujących parametrów linii: * mapa połączeń, ciągłość przewodów (wire map, continuity of conductors), * długość (Length), * rezystancja ( DC Loop Resistance), * opóźnienie propagacji (Propagation Delay), * skośne opóźnienie propagacji (Delay Skew), * osłabienie sygnału częścią odbitą (Return Loss), * tłumienność (Attenuation), * przesłuch para-para na tym samym końcu kabla (Near End Crosstalk - NEXT), * stosunek tłumienności do przesłuchu (Attenuation to Crosstalk Ratio - ACR), * suma przesłuchów para-pozostałe 3 pary (Power Sum NEXT - PSNEXT), * równoważony przesłuch para-para na przeciwległych końcach kabla (Equal Level Far End Crosstalk – ELFEXT), * suma równoważonych przesłuchów para-pozostałe 3 pary na przeciwległych końcach kabla (Power Sum Equal Level Far End Crosstalk – PSELFEXT), * stosunek tłumienności do sumy przesłuchów (Power Sum ACR – PSACR). * Wyniki pomiarów dynamicznych wykonane miernikiem okablowania powinny zostać zamieszczone w formie wydruków w dokumentacji powykonawczej. * **Dostosowanie istniejącej sieci elektrycznej do punktów dystrybucyjnych:** * Wykonawca wykona fizyczne przyłączenie zasilania w punktach dystrybucyjnych, (jeżeli będzie taka potrzeba). * Dla każdego punktu dystrybucyjnego Wykonawca wykona prace polegające na dociągnięciu zasilania z najbliższego punktu rozdzielczego lub wydzielonego przyłącza dla urządzeń informatycznych. * Dedykowana sieć elektryczna może nie być scentralizowana i wyprowadzana z tablicy głównej danego budynku lub danej kondygnacji. * Wykonawca uzgodni z Zamawiającym warunki odnośnie zasilania elektrycznego (ilość istniejących i dopuszczalnych obudów elektrycznych oraz ich lokalizacje w punktach przyłączeniowych). * Każdy z przygotowywanych obwodów musi zawierać odpowiednie zabezpieczenia (w szczególności różnicowo-prądowe, przepięciowe oraz nadprądowe). * W przypadku, kiedy istniejące warunki energetyczne dla lokalizacji (przyłącza energetycznego do budynku) po uwzględnieniu zapotrzebowania energetycznego generowanego przez dostarczaną infrastrukturę okażą się niewystarczające, Wykonawca przygotuje niezbędne dokumenty do uzyskania wymaganych warunków energetycznych od dystrybutora energii. * **Demontaż i utylizacja dotychczasowego okablowania wraz z punktami dystrybucyjnymi:** * Jeżeli zaistnieje taka potrzeba Wykonawca za zgodą i akceptacją Zamawiającego zobowiązuje się do zdemontowania i utylizacji istniejącego (starego) okablowania strukturalnego oraz elektrycznego. * Miejsca po demontażu powinny zostać naprawione i zamalowane farbą w kolorze uzgodnionym z Zamawiającym. * **Termin realizacji:** * Powyższe czynności należy wykonać w okresie realizacji Zamówienia, po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym. * Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w siedzibie Zamawiającego w pierwszym dniu roboczym następującym po pracach wdrożeniowo-instalacyjnych w godzinach od 7.00 do 15.00. * Zamawiający wymaga, aby na wezwanie (oferta wygrywająca) dostarczyć karty katalogowe głównych elementów systemu np.: wykorzystywane okablowanie, patchpanele, gniazda RJ45. * **Opracowanie dokumentacji powykonawczej:** * Po zakończeniu robót Wykonawca zobowiązany jest przedłożyć Zamawiającemu dokumentację powykonawczą zawierającą mapy w skali 1:100 z dołączonymi pomiarami i testami sieci komputerowej oraz instalacji elektrycznej oraz opisem wykonanej instalacji. Dokumentacja powykonawcza powinna zawierać projekt sieci komputerowej, instalacji elektrycznej, z naniesionymi punktami dostępowymi wraz z przebiegiem trasy kablowej w pomieszczeniach Zamawiającego; powinna zawierać również zestawienie materiałów użytych do jej wykonania. * Wymagana jest forma papierowa i elektroniczna dokumentacji, zatwierdzona przez osoby z odpowiednimi uprawnieniami (uprawnienia producenta okablowania do projektowania okablowania strukturalnego). * Dokumentacja powinna zawierać konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania, które nie umożliwiają wyeksportowanie konfiguracji do pliku tekstowego bądź posiadają rozproszoną konfigurację). * Dokumentacja powinna zawierać pliki pomiarów komputerowych, które muszą być nieprzetworzonymi plikami pobranymi bezpośrednio z miernika pomiarowego. * Certyfikat producenta okablowania strukturalnego dla projektowanej kategorii/klasy, wyniki pomiarów dla wszystkich linii okablowania (wydruk z miernika), certyfikaty dopuszczenia do obrotu na użyte komponenty w instalacji (dostarcza producent lub przedstawiciel regionalny). * **GWARANCJA**   Całość rozwiązania ma być objęta jednolitą, spójną 25-letnią gwarancją systemową producenta, obejmującą całą część transmisyjną wraz z kablami krosowymi i innymi elementami dodatkowymi. Gwarancja ma być udzielona przez producenta bezpośrednio klientowi końcowemu.  25-letnia gwarancja systemowa ma być bezpłatną usługą serwisową oferowaną użytkownikowi końcowemu przez producenta okablowania. Musi obejmować ona swoim zakresem całość systemu okablowania od głównego punktu dystrybucyjnego do gniazda użytkownika i zawierać, podsystem okablowania szkieletowego i poziomego.  W celu uzyskania tego rodzaju gwarancji cały system musi być zainstalowany przez firmę instalacyjną posiadającą odpowiedni status uprawniający do udzielenia gwarancji producenta. Wniosek o udzielenie gwarancji składany przez firmę instalacyjną do producenta ma zawierać: listę zainstalowanych elementów systemu, wyciąg z dokumentacji powykonawczej podpisany przez projektanta oraz instalatora, wyniki pomiarów dynamicznych typu Permanent Link wszystkich torów transmisyjnych według norm ISO/IEC 11801 ed. 2.2 lub EN 50173-1 (lub równoważnych). **Aby na etapie oferty dowieść zdolności udzielenia gwarancji 25-letniej systemowej producenta systemu okablowania –** **firma instalacyjna winna przedstawić na wezwanie Zmawiającego- certyfikat imienny zatrudnionego pracownika wydany przez producenta (a nie w imieniu producenta).** |