Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia

NR REF. TARRSA/IT/1/2019

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV)

48800000-6 - Systemy i serwery informacyjne

72415000-2 - Usługi hostingowe dla stron WWW

72317000-0 - Usługi przechowywania danych

[72253200 - Usługi w zakresie wsparcia systemu](https://www.portalzp.pl/kody-cpv/szczegoly/uslugi-w-zakresie-wsparcia-systemu-8438)

[72611000 - Usługi w zakresie wsparcia technicznego](https://www.portalzp.pl/kody-cpv/szczegoly/uslugi-w-zakresie-wsparcia-technicznego-8502)

Przedmiotem zamówienia jest usługa zapewnienia dostępu do bezpiecznej i wysokodostępnej infrastruktury informatycznej w modelu usługowym wraz z usługami uzupełniającymi i obsługą informatyczną.

Usługa składa się z „Usługi podstawowej” oraz „Usług dodatkowych”.

W ramach realizacji Usługi Wykonawca musi udostępnić powierzchnię w centrum przetwarzania danych, sprzęt i oprogramowanie zgodnie z określonymi przez Zamawiającego wymaganiami. Ponadto musi zapewnić łącza do sieci Internet, dedykowane łącze/a do ośrodka przetwarzania danych u Zamawiającego, infrastrukturę teletechniczną wraz z niezbędnymi urządzeniami, oprogramowaniem i licencjami potrzebnymi do uruchomienia i prawidłowego działania Usługi zgodnie z określonymi parametrami. Wykonawca musi zapewnić obsługę udostępnionego sprzętu i oprogramowania wraz ze wsparciem administratorów, ochronę przed atakami i instalacją złośliwego oprogramowania oraz zapewnić mechanizmy i narzędzia do zbierania i przechowania logów zdarzeń z urządzeń styku z siecią Internet (syslog). Wykonawca musi zapewnić stałą obsługę wsparcia administracyjnego oraz obsługi informatycznej typ helpdesk w siedzibie Zamawiającego.

Wykonawca zapewni bezpieczeństwo informacji, w tym danych osobowych, przetwarzanych w ramach sieci i systemów informatycznych polegające na zagwarantowaniu ich dokładności i kompletności oraz zapewni poufność, integralność i dostępność danych wyłącznie dla autoryzowanych osób, potwierdzone posiadaniem kompletnych i wysoko dostępnych rozwiązań opartych o najwyższe standardy bezpieczeństwa informacji oraz posiadanie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą ISO 27001 lub porównywalnego systemu o standardach nie niższych niż wskazana norma.

Wykonawca zapewni ciągłość działania obsługi poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych umożliwiających bezpieczne utrzymanie i eksploatację systemu informacyjnego oraz zapewni właściwe reagowanie, w trakcie zaistnienia incydentu zaburzającego ciągłość działania, potwierdzone posiadaniem kompletnych i wysoko dostępnych rozwiązań opartych o najwyższe standardy ciągłości działania oraz posiadanie Systemu Zarządzania Ciągłością Działania zgodnego z normą ISO 22301 lub porównywalnego systemu o standardach nie niższych niż wskazana norma.

**1. Wymagania dla ośrodka centrum przetwarzania danych (CPD)**

Z uwagi na potrzebę wysokiej dostępności oferowanych usług Zamawiający oczekuje aby proponowane rozwiązanie spełniało najwyższe standardy bezpieczeństwa informatycznego.

Wymagania dla centrum przetwarzania danych w którym gromadzone będą dane będące przedmiotem postepowania. Wszystkie wymagania są obligatoryjne. Wykonawca spełnia wymogi na zasadzie „Tak” lub „Nie”.

Tabela nr 1. Centrum przetwarzania danych.

|  |  |  |  |
| --- | --- | --- | --- |
| OBIEKT I LOKALIZACJA | | | |
| L.p. | Parametr lub kryterium | Wyeliminowanie zagrożenia | Wykonawca spełnia  (TAK / NIE) |
| 1 | Centrum przetwarzania danych zlokalizowane na terenie na terenie UE lub Lichtenstainu, Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na terenie UE lub Lichtenstainu, Islandii, Norwegii. | Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR. |  |
| 2 | Ogrodzony teren centrum przetwarzania danych. | Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka. |  |
| 3 | Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie. | Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury. |  |
| 4 | Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej | Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych. |  |
| 5 | Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych. | Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko). |  |
| 6 | Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób). | Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń. |  |
| 7 | Minimum 200 m oddalenie od linii wysokiego napięcia i elektrowni. | Zagrożenie spowodowania uszkodzeń wynikających z awarii linii wysokiego napięcia, ryzyko wybuchów, ryzyko pożarów. Zagrożenie długotrwałego ograniczenia dostępu do ośrodka wynikającego z wykonywanych napraw. |  |
| 8 | Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami. | Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności). |  |
| 9 | Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Zamawiającemu od źródeł pól zakłócających (transformatory SN i WN). | Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pół zakłócających pracę urządzeń elektrycznych i magnetycznych. |  |
| 10 | Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu | Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych. |  |
| 11 | Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m | Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych. |  |
| 12 | Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1. | Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych. |  |
| 13 | Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej. | Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej. |  |
| WĘZŁY TELEKOMUNIKACYJNE | | | |
| 1 | Podłączenie w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym | Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora. |  |
| 2 | Dojścia połączeń do ośrodka wykonane dwoma niezależnymi trasami kablowymi. | Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem. |  |
| 3 | Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP | Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet. |  |
| 4 | Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99% | Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet. |  |
| 5 | Węzeł telekomunikacyjny wyposażony w redundantny system firewall | Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej. |  |
| 6 | Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci. | Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy. |  |
| ZASILANIE | | | |
| 1 | Dostępność roczna systemu zasilania 99,99% | Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń. |  |
| 2 | Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT | Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania. |  |
| 3 | System zasilania awaryjnego UPS osobno na każdą linię zasilającą | Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego. |  |
| 4 | Redundantny system agregatów prądotwórczych | Zagrożenie braku zachowania zasilania |  |
| 5 | System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną | Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów. |  |
| 6 | Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy. | Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów. |  |
| BEZPIECZEŃSTWO | | | |
| 1 | Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 dni, system kontroli dostępu (SKD). | Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urządzeń. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urządzeń. |  |
| 2 | Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania. | Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu. |  |
| 3 | Ochrona przez zewnętrzną licencjonowaną firmę. | Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej. |  |
| 4 | System CCTV zapewnia ciągły 365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne. | Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób. |  |
| 5 | System CCTV powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres co najmniej 21 dni. | Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń. |  |
| 6 | System SKD dzieli centrum przetwarzania danych wraz z terenem na minimum IV strefy dostępu z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku. |  |
| 7 | Dostęp do strefy I (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów). | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |  |
| 8 | Dostęp do strefy II (część administracyjno-biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |  |
| 9 | Dostęp do strefy III (strefa technologiczna) możliwy wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |  |
| 10 | Dostęp do strefy IV (pomieszczenia ze sprzętem komputerowym Zamawiającego) możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |  |
| 11 | System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego. | Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia. |  |
| 12 | Ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej. | Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru. |  |
| MONITOROWANIE | | | |
| 1 | System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7 | Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej. |  |
| 2 | Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności. | Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń. |  |

Ośrodek przetwarzania musi posiadać zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo danych przetwarzanych. Ośrodek ponosi odpowiedzialność w zakresie bezpieczeństwa informacji przechowywanych na wykorzystanej infrastrukturze serwerowej.

Tabela 2. Bezpieczeństwo sprzętu informatycznego.

|  |  |  |
| --- | --- | --- |
|  | Zakres | Wykonawca spełnia  (TAK / NIE) |
| 1 | Izolacja sprzętu krytycznego |  |
| 2 | Ochrona przed uszkodzeniem |  |
| 3 | Rejestr wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego |  |
| 4 | Ochrona przed dostępem dla osób nieupoważnionych |  |

Tabela 3. Naprawy i konserwacja sprzętu.

|  |  |  |
| --- | --- | --- |
|  | Zakres | Wykonawca spełnia  (TAK / NIE) |
| 1 | Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu. |  |
| 2 | Obsługa i naprawy muszą być dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami Ośrodka. |  |
| 3 | Należy usuwać nośniki danych przed przekazaniem sprzętu do naprawy. |  |
| 4 | Należy stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi). |  |
| 5 | Należy wykonywać przeglądy techniczne zgodnie z wymaganiami producenta sprzętu i procedurami wewnętrznymi Ośrodka. |  |
| 6 | Należy chronić Zamawiającego przed instalacją złośliwego oprogramowania. |  |
| 7 | Należy prowadzić rejestr incydentów, awarii i usterek. |  |
| 8 | Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu. |  |

**2. Warunki ciągłości działania SLA i czas reakcji**

1. SLA dla świadczonej usługi serwerów wirtualnych i usług SaaS wynosi minimum 99,95% w skali miesiąca.
2. Obsługa zarządzania serwerami wirtualnymi musi być realizowana w trybie 24/7/365.
3. Obsługa help desk musi być realizowana w trybie 8/5 w godzinach 8.00-16.00.
4. Czas reakcji na zgłoszenie musi wynosić do 60 min od przyjęcia zgłoszenia.
5. Czas realizacji zgłoszenia musi wynosić do 12h od przyjęcia zgłoszenia.

**3. Uruchomienie usługi**

W ramach uruchomienia Usługi Wykonawca jest zobowiązany:

1. udostępnić Zamawiającemu maszyny wirtualne gotowe do instalacji aplikacji i serwisów zamawiającego;
2. zainstalować na maszynach wirtualnych systemy operacyjne (wraz z zapewnieniem niezbędnej ilości licencji);
3. zainstalować na maszynach wirtualnych oprogramowanie bazodanowe wraz z zapewnieniem niezbędnej ilości licencji;
4. skonfigurować połączenia sieciowe pomiędzy poszczególnymi maszynami wirtualnymi;
5. skonfigurować i udostępnić dedykowane łącze/a do siedziby Zamawiającego zgodnie z określonymi parametrami;
6. skonfigurować i udostępnić łącze do sieci Internet, zgodnie z określonymi parametrami;
7. skonfigurować ochronę na styku z Internetem w warstwie sieciowej i aplikacyjnej;
8. zapewnić niezbędne licencje, sprzęt związane z realizacją umowy;
9. skonfigurować i udostępnić system do wykonywania kopii bezpieczeństwa wszystkich serwerów i bazy danych;
10. skonfigurować i udostępnić system zbierania i przechowania logów zdarzeń z urządzeń styku z siecią Internet.
11. świadczyć usługę administrowania uruchomionymi maszynami wirtualnymi do poziomu systemu operacyjnego, zgodnie z określonymi parametrami;
12. świadczyć obsługę wsparcia typu helpdesk, zgodnie z określonymi parametrami.
13. **Usługa podstawowa**

**4.1. Serwery wirtualne**

W ramach realizacji Usługi Wykonawca musi udostępniać maszyny wirtualne oraz oprogramowanie systemowe i narzędziowe o parametrach nie gorszych niż obecnie wykorzystywane przez Zamawiającego określone w Tabeli 1. Wykonawca musi zapewnić niezawodność i ciągłość pracy serwerów wirtualnych (wysoką dostępność). W przypadku awarii serwera fizycznego musi następować automatyczne przełączenie urządzeń w celu utrzymania ciągłości pracy zasobów. Wykonawca musi zapewnić migrację z obecnych serwerów wirtualnych Zamawiającego i ich konfigurację w środowisku Wykonawcy. Wymagana jest regularna realizacja usługi backupowej całego środowiska serwerów wirtualnych (1 kopia raz dziennie, retencja 7 dni) w trakcie całego czasu trwania umowy. Wymagany jest monitoring środowiska w zakresie wydajności (zajętość dysków, dostępność usług, ważność certyfikatów) w trakcie całego czasu trwania umowy.

Tabela 4. Parametry techniczne serwerów wirtualnych

|  |  |  |
| --- | --- | --- |
| 1 | Serwery (www) x 1 | Minimalne wymagania Zamawiającego |
| a | Architektura | x86-64 |
| b | Pamięć podstawowa | 4 GB DDR3 1333MHz |
| c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |
| d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |
| e | Interfejsy sieciowe | 2 x 1Gb |
| f | Moduł zarządzania | Wymagany |
| g | System operacyjny | CentOS z możliwością upgrade do nowszej wersji lub równoważny |
| h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |
| i | Adres zewnętrzny | 3 x IPv4 |
| 2 | Serwery (plików) x 2 | Minimalne wymagania Zamawiającego |
| a | Architektura | x86-64 |
| b | Pamięć podstawowa | 4 GB DDR3 1333MHz |
| c | Procesor/Procesory | 4 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |
| d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |
| e | Interfejsy sieciowe | 2 x 1Gb |
| f | Moduł zarządzania | Wymagany |
| g | System operacyjny | Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny |
| h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |
| i | Przestrzeń dyskowa | 3000 GB (5.000 IOPS) |
| 3 | Serwery (aplikacja) x 2 | Minimalne wymagania Zamawiającego |
| a | Architektura | x86-64 |
| b | Pamięć podstawowa | 4 GB DDR3 1333MHz |
| c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |
| d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |
| e | Interfejsy sieciowe | 2 x 1Gb |
| f | Moduł zarządzania | Wymagany |
| g | System operacyjny | Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny |
| h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |
| 4 | Serwery (generator) x2 | Minimalne wymagania Zamawiającego |
| a | Architektura | x86-64 |
| b | Pamięć podstawowa | 2 GB DDR3 1333MHz |
| c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |
| d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |
| e | Interfejsy sieciowe | 2 x 1Gb |
| f | Moduł zarządzania | Wymagany |
| g | System operacyjny | CentOS z możliwością upgrade do nowszej wersji lub równoważny |
| h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |
| 5 | Serwery (AD) x 2 | Minimalne wymagania Zamawiającego |
| a | Architektura | x86-64 |
| b | Pamięć podstawowa | 4 GB DDR3 1333MHz |
| c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |
| d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |
| e | Interfejsy sieciowe | 2 x 1Gb |
| f | Moduł zarządzania | Wymagany |
| g | System operacyjny | Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny |
| h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |
| 6 | Serwery (OCS) x 1 | Minimalne wymagania Zamawiającego |
| a | Architektura | x86-64 |
| b | Pamięć podstawowa | 2 GB DDR3 1333MHz |
| c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |
| d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |
| e | Interfejsy sieciowe | 2 x 1Gb |
| f | Moduł zarządzania | Wymagany |
| g | System operacyjny | CentOS z możliwością upgrade do nowszej wersji lub równoważny |
| h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |
| 6 | Serwery (Update) x 1 | Minimalne wymagania Zamawiającego |
| a | Architektura | x86-64 |
| b | Pamięć podstawowa | 2 GB DDR3 1333MHz |
| c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |
| d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |
| e | Interfejsy sieciowe | 2 x 1Gb |
| f | Moduł zarządzania | Wymagany |
| g | System operacyjny | Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny |
| h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |

Tabela 5. Podsumowanie ilości komponentów serwerów wirtualnych

|  |  |  |
| --- | --- | --- |
|  | Komponent | Ilość |
| 1 | Razem serwery wirtualne | 11 szt. |
| 2 | Rezem Pamięć podstawowa - DDR3 1333MHz | 36 GB |
| c | Razem procesory - 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 | 26 vCPU |
| d | Razem system operacyjny - CentOS z możliwością upgrade do nowszej wersji lub równoważny | 4 szt. |
| e | Razem system operacyjny - Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny | 7 szt. |
| f | Razem adres zewnętrzny IPv4 | 3 szt. |
| g | Razem sieć wewnętrzna vLAN | 11 szt. |
| h | Razem przestrzeń dyskowa 5000 IOPS | 7100 GB |

Tabela 6. Opisy równoważności:

|  |  |
| --- | --- |
| Windows Server 2016 | Minimalne funkcjonalności:   1. możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; 2. możliwość dokonywania uaktualnień sterowników urządzeń przez Internet witrynę producenta systemu; 3. darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat); 4. wymagane podanie nazwy strony serwera www; 5. internetowa aktualizacja zapewniona w języku polskim; 6. wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami ip v4 i v6; 7. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe; 8. możliwość uruchomienia kontrolera domeny będącego w pełni zgodnym z wdrożoną u Zamawiającego domeną AD pracującą w oparciu o system Windows Server 2012 R2 (poziom funkcjonalności AD DS Windows Server 2012 R2); 9. możliwość uruchomienia kontrolera domeny tylko do odczytu; 10. możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny i w pełni zgodnego z serwerami DNS Zamawiającego pracującymi w oparciu Windows Server 2012 R2 Enterprise; 11. możliwość uruchomienia serwera usług terminalowych (RemoteApp) zgodnego z Windows Server 2012 R2; obsługa zdalnego pulpitu; 12. możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 13. obsługa wirtualizatora Hyper-V 14. obsługa PowerShell 4.0 15. obsługa certyfikatów w AD; 16. obsługa Microsoft Office 2013; 17. obsługa drzewa katalogowego Microsoft Active Directory. |
| CentOS | 1. System operacyjny z bezpośrednim wsparciem producenta 24x7 przez okres min. 1 roku z możliwością późniejszego rozszerzenia okresu wsparcia technicznego. Licencja nie może być przypisana do konkretnej maszyny i musi umożliwiać przenoszenie oprogramowania między różnymi serwerami. 2. Wsparcie producenta systemu operacyjnego realizowane jest w trybie 24x7 z gwarantowanym czasem reakcji na zgłaszane problemy do 1 godziny dla pytań krytycznych oraz bez ograniczeń dotyczących ilość zgłoszeń w miesiącu. Wsparcie techniczne realizowane jest przez kanały – telefon/web/email. 3. System operacyjny jest standardowo wyposażony w mechanizm bezpieczeństwa Security Enhanced Linux (SELinux) wraz z przygotowanymi i uaktualnionymi politykami bezpieczeństwa. System zapewnia narzędzia tekstowe i graficzne pozwalające w prosty sposób analizować alarmy bezpieczeństwa. 4. System operacyjny posiada wbudowaną obsługę wirtualizacji oraz narzędzia tekstowe i graficzne służące do zarządzania maszynami wirtualnymi. 5. System operacyjny z wbudowaną obsługą wirtualizacji umożliwia uruchomienie nieograniczonej liczby wirtualnych maszyn. 6. Instalator systemu operacyjnego umożliwia utworzenie szyfrowanych partycji jeszcze przed instalacją systemu operacyjnego. |

**4. 2. Administrowanie serwerami**

Do zadań realizowanych przez Wykonawcę w ramach usług utrzymaniowych infrastruktury informatycznej i wsparcia IT należy bieżąca obsługa administracyjna zasobów informatycznych (serwerów wirtualnych) wraz z nadzorem nad posiadaną przez Zamawiającego infrastrukturą zlokalizowaną w centrum przetwarzania danych, składającą się w szczególności z zasobów IaaS (Infrastructure as a Service) oraz PaaS (Platform as a Service), poprzez świadczenie usług informatycznych w zakresie:

1. migracji usług do infrastruktury cloud i ich utrzymania;
2. instalacji i konfiguracji systemów operacyjnych;
3. instalacji i konfiguracji elementów niezbędnych do zapewnienia środowiska wysokiej dostępności (HA);
4. aktualizacji oprogramowania ze względu na błędy bezpieczeństwa;
5. utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa;
6. realizacji bieżących czynności administracyjnych;
7. realizacji polityki kopii zapasowych gromadzonych danych;
8. utrzymania infrastruktury sieciowej (urządzenia sieciowe, punkty AP, połączenia VPN);
9. konsultacji wykonawczych z użytkownikami wewnętrznymi i zewnętrznymi;
10. świadczenia usług doradczych m.in. poprzez udział w pracach związanych z zakupami sprzętu komputerowego, oprogramowania, licencji oraz kontraktów serwisowych;
11. analiz incydentów oraz problemów wraz pełnym przywracaniem funkcjonalności.

**4.3. Obsługa Helpdesk**

Do zadań realizowanych przez Wykonawcę należy świadczenie usług w zakresie help desk w siedzibie Zamawiającego, tj. w budynek „G” na terenie Toruńskiego Parku Technologicznego, ul Włocławska 167. Zakres przedmiotu obsługi obejmuje:

1. przyjmowanie zgłoszeń w trybie 24/7/365 w systemie online (dedykowane narzędzie z historią zgłoszeń, statusem zgłoszenia);
2. diagnozowanie problemów, konfiguracji ustawień i sterowników, zamawiania usług serwisu zewnętrznego drukarek biurowych (maksymalna ilość obsługiwanych drukarek 10 szt.);
3. obsługę materiałów eksploatacyjnych, diagnozowania problemów, konfiguracji ustawień i sterowników, zamawiania usług serwisu zewnętrznego drukarek centralnych (maksymalna ilość obsługiwanych drukarek 4 szt.);
4. diagnozowanie problemów, konfiguracji, instalacji oprogramowania, optymalizacji wydajności urządzeń końcowych (komputery stacjonarne, laptopy, tablety) w ilości co najmniej jednego urządzenia na każdego pracownika oraz dodatkowo jednego urządzenia przypisanego do każdego Działu wg. struktury organizacyjnej Zamawiającego (łącznie do 60 urządzeń końcowych);
5. prowadzenie aktualnego rejestru użytkowanego sprzętu wyposażenia IT użytkowanego przez Zamawiającego (komputery stacjonarne, komputery przenośne, tablety, wykorzystywane licencje);
6. zarządzanie kluczowymi licencjami, w tym. m.in.: MS Windows, MS Office, Enova, Symfonia, oprogramowanie antywirusowe (monitorowanie ilości, aktywacja, aktualizacja);
7. konfiguracje i instalacje nowych stanowisk pracy (instalacja i konfiguracja oprogramowania, aktywacja usług zgodnie z polityką firmy – poczta, backup, usługi backoffice);
8. usuwanie i archiwizacje danych, w tym likwidowanych stanowisk pracy, formatowanie urządzeń końcowych oraz zarządzenie uprawnieniami;
9. obsługę i aktualizację zabezpieczeń stron www z wykorzystaniem WordPress;
10. monitoring, rejestrację i przedłużanie posiadanych domen internetowych;
11. rekonfigurację użyteczności Sharepoint zgodnie z przedstawionymi wytycznymi;
12. konfigurację, diagnostykę, rozbudowy i modyfikacji logicznych sieci komputerowych odpowiedzialnych za prawidłowe działanie sieci Internet w obiektach Zamawiającego na terenie Toruńskiego Parku Technologicznego;
13. konsultację w zakresie określenia parametrów technicznych dla nowo kupowanego sprzętu IT, oprogramowania oraz drukarek biurowych.

**4.4 Poczta email**

Dostawa, wdrożenie i utrzymanie usługi poczty email w modelu SaaS – 60 kont pocztowych.

Tabela nr 7. Wymagania dotyczące poczty email.

|  |  |
| --- | --- |
| Lp. | Minimalne wymagania |
| 1 | Powierzchnia dysku pojedynczego użytkownika 10 GB |
| 2 | Maksymalny rozmiar załącznika w jednej wiadomości email 40 MB |
| 3 | Środowisko MS Exchange 2016 |
| 4 | Dostęp do OWA (Outlook Web Aplication) |
| 5 | ActiveSync dla smartfonów i tabletów |
| 6 | Dostęp przez IMAP |
| 7 | Integracja z firmowym Active Directory |
| 8 | Ochrona antyspamowa i antywirusowa na serwerze |
| 9 | Własna domena firmowa |
| 10 | MS Outlook 2016 |
| 11 | Prywatny i współdzielony kalendarz |

**4.5. Ochrona antywirusowa**

Dostawa, wdrożenie i utrzymanie usługi ochrony antywirusowej i antymalware’owej stacji roboczych wraz z zabezpieczeniem skrzynek pocztowych – 60 stacji roboczych.

Tabela nr 8. Wymagania dotyczące ochrony antywirusowej i antymalware’owej

|  |  |
| --- | --- |
| Lp. | Minimalne wymagania |
| 1 | Systemy Operacyjne Komputerów  ● Windows 10 Anniversary Update "Redstone"  ● Windows 10 TH2  ● Windows 10  ● Windows 8.1  ● Windows 8  ● Windows 7  ● Windows Vista z dodatkiem Service Pack 1  ● Windows XP z Service Pack 2 64 bit  ● Windows XP z Service Pack 3  Tablety i Wbudowane Systemy Operacyjne  ● Windows Embedded 8.1 Industry  ● Windows Embedded 8 Standard  ● Windows Embedded Standard 7  ● Windows Embedded Compact 7  ● Windows Embedded POSReady 7  ● Windows Embedded Enterprise 7  ● Windows Embedded POSReady 2009  ● Windows Embedded Standard 2009  ● Windows XP z wbudowanym Service Pack 2  ● Windows XP Tablet PC Edition |
| 2 | Systemy Operacyjne Mac OS X  ● Mac OS X Sierra (10.12.x)  ● Mac OS X El Capitan (10.11.x)  ● Mac OS X Yosemite (10.10.5)  ● Mac OS X Mavericks (10.9.5)  ● Mac OS X Mountain Lion (10.8.5) |
| 3 | Wymagania Ochrony Mobile  ● Apple iPhone i tablety iPad (iOS 5.1+)  ● Smartfony i tablety z Google Android (2.3+) |
| 4 | Obsługiwane Środowiska Microsoft Exchange  ● Exchange Server 2016 z rolą Edge Transport  lub Mailbox  ● Exchange Server 2013 z rolą Edge Transport  lub Mailbox  ● Exchange Server 2010 z rolą Edge Transport,  Hub Transport lub Mailbox  ● Exchange Server 2007 z rolą Edge Transport,  Hub Transport lub Mailbox |
| 5 | Wymagania funkcjonalno-użytkowe:   1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 4. Wbudowana technologia do ochrony przed rootkitami. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 8. Możliwość skanowania dysków sieciowych i dysków przenośnych. 9. Skanowanie plików spakowanych i skompresowanych. 10. Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów. 11. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express. 12. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 13. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 14. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 15. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. 16. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 17. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS. 19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 20. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło. 21. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie” możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony. 22. Możliwość pobrania płyty ratunkowej, do uruchomienia z niej komputera i przeskanowania dysków umieszczonych w komputerze. 23. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 24. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym. 25. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 27. Praca programu musi być niezauważalna dla użytkownika. 28. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. 29. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. 30. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 31. Możliwość odblokowania ustawień programu po wpisaniu hasła 32. Posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu modułu Super użytkownika 33. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie) 34. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów. 35. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp. 36. Funkcja Ochrony danych konfigurowana zdalnie przez administratora. 37. Jedna wersja instalacyjna na stacje robocze i serwery plików. 38. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 39. Możliwość zainstalowania silnika pełnego, lekkiego z sprawdzaniem reputacji plików w chmurze, lub skanowanie przez centralny serwer bezpieczeństwa. 40. Możliwość tworzenia list sieci zaufanych. 41. Możliwość dezaktywacji funkcji zapory sieciowej. 42. Możliwość ochrony systemu bez instalacji na stacji roboczej silnika antywirusowego. Jego role przejmuje centralny serwer bezpieczeństwa odpowiedzialny za proces skanowania plików. 43. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 44. Dodatkowy moduł ochrony przeciwko zagrożeniom typu ransomware |
| 6 | Urządzenia Mobilne   1. Dla systemu Android możliwość blokowania stron internetowych. 2. Możliwość szyfrowania urządzenia opartego o system android. 3. Możliwość pobrania wersji instalacyjnej ze sklepu iOS oraz Android 4. Skanowanie aplikacji w trakcie instalacji na urządzeniach z systemem Android 5. Posiadać możliwość szyfrowania urządzenia dla systemu Android 6. Ochrona stron internetowych dla androida pod kontem malware, exploit, phishing 7. Możliwość blokowania ekranu głównego hasłem. 8. Możliwość definiowania i zabezpieczania połączeń WiFi 9. Dla systemu Android moduł odpowiedzialny za blokowanie stron. 10. Kontrola przeglądarki Safari dla urządzeń z systemem iOS |

**4.6. Usługa katalogowa**

Dostawa, wdrożenie i utrzymanie usługi katalogowej (Microsoft Share Point lub równoważny) w oparciu o jednolity system uprawnień z przestrzenią 20 GB dla użytkownika końcowego Zamawiającego - 60 użytkowników.

Tabela nr 9. Tabela równoważności.

|  |  |
| --- | --- |
| Microsoft Share Point | Warunki jakie musi spełniać dostarczany serwer systemu wyszukiwania i gromadzenia danych aby został uznany za równoważny (Microsoft SharePoint 2010).  Serwer systemu wyszukiwania i gromadzenia danych (SWGD) musi zapewniać:   1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych i zewnętrznych. 2. Zarządzanie strukturą portalu i treściami WWW. 3. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej. 4. Udostępnienie formularzy elektronicznych. 5. Tworzenie repozytoriów wzorów dokumentów. 6. Tworzenie repozytoriów dokumentów. 7. Wspólną, bezpieczną pracę nad dokumentami. 8. Wersjonowanie dokumentów (dla wersji roboczych). 9. Organizację pracy grupowej. 10. Wyszukiwanie treści. 11. Dostęp do danych w relacyjnych bazach danych. 12. Analizę danych wraz z graficzną prezentacją danych. 13. Możliwość wykorzystania mechanizmów portalu do budowy systemu zarządzania eszkoleniami (e-learning). 14. Możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie. 15. Mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.   Serwery SWGD muszą posiadać następujące cechy dostępne bezpośrednio, jako wbudowane właściwości produktu:   1. Interfejs użytkownika:    1. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).    2. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0.    3. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów.    4. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego.    5. Możliwość pracy off-line z plikami przechowywanymi w repozytoriach portalu.    6. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy). 2. Uwierzytelnianie – wbudowane mechanizmy wspierające uwierzytelnianie na bazie:    1. Oświadczeń (claim-based authentication) z wykorzystaniem:       1. Open Authorization 2.0 dla uwierzytelniania aplikacji,       2. Uwierzytelniania w trybie server-to-server,       3. SAML iv. Windows claims.    2. Pojedynczego logowania domenowego (single-sign on).    3. Na bazie formularzy (Form-based). 3. Projektowanie stron:    1. Wbudowane intuicyjne narzędzia projektowania wyglądu stron.    2. Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML.    3. Wsparcie dla ASP.NET, Apache, C#, Java i PHP.    4. Możliwość osadzania elementów iFrame w polach HTML na stronie. 4. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:    1. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili.    2. Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów.    3. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili.    4. Integracja z systemem obsługującym serwis WWW w zakresie publikacji treści z repozytoriów wewnętrznych firmy na zewnętrzne strony serwisu WWW (pliki, strony).    5. Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego.    6. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services.    7. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.    8. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych. 5. Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej przez autorów treści:    1. Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania.    2. Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów publikowanych w intranecie (stron HTML).    3. Spójne zarządzanie wyglądem stron intranetu, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego.    4. Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron intranetu i przechowywanymi w intranetowym repozytorium treści. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów.    5. Definiowanie szablonów dla układów stron (tzw. layout’ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach intranetu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte.    6. Możliwość wielokrotnego wykorzystania elementów zawartości intranetu (części treści publikowanych na stronach) w różnych częściach portalu, tzn. modyfikacja zawartości w jednym miejscu powoduje jej faktyczną zmianę na wszystkich stronach intranetu, gdzie dana treść została opublikowana    7. Możliwość odwzorowania w systemie CMS przyjętej wizualizacji portalu intranetowego (projekt graficzny i funkcjonalny).    8. Możliwość osadzania na stronach narzędzia do odtwarzania materiałów audio i wideo, 6. Organizacja i publikacja treści:    1. Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści.    2. Zastosowanie procesów zatwierdzania zawartości przez publikacją, tzn. Udostępnieniem jej dla szerokiego grona pracowników. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed Udostępnieniem jej wszystkim użytkownikom intranetu.    3. Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji.    4. Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące obecną hierarchię.    5. Automatyczne generowanie mapy stron portalu.    6. Możliwość definiowania nawigacji w oparciu o centralne zarządzanie metadanymi.    7. Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu.    8. Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do odczytu zawartości, jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT.    9. Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji.    10. Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości, i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji.    11. Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu oraz zapewnienie automatycznego tłumaczenia na wybrane języki. 7. Repozytoria dokumentów:    1. Możliwość prostej publikacji dokumentów w intranecie przez edytorów portalu. Prosty sposób publikacji dokumentów, funkcjonalny dostęp użytkowników intranetu do opublikowanych dokumentów.    2. Wykorzystanie do publikacji, edycji i przeglądania dokumentów w repozytorium narzędzi znanych użytkownikom np. pakiety biurowe czy przeglądarka internetowa.    3. Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu.    4. Możliwość publikacji plików w strukturze katalogów.    5. Możliwość publikacji materiałów wideo oraz audio.    6. Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku.    7. Możliwość nawigacji po repozytorium dokumentów (lub całym portalu) w oparciu o metadane z metryk dokumentów.    8. Prosty, elastyczny i niezależny od działu IT mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania.    9. Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x… 2.0), automatyczna kontrola wersji przy publikacji dokumentów.    10. Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub modyfikowanych dokumentów. System informuje użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i pozwala podjąć decyzję o ich publikacji lub odrzuceniu.    11. Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych.    12. Możliwość definiowania polityk cyklu życia dokumentu oraz retencji dokumentów.    13. Możliwość tworzenia specjalnych repozytoriów przeznaczonych na raporty osadzone w arkuszach kalkulacyjnych w formacie ISO/IEC 29500:2008. Serwer powinien generować na podstawie tych arkuszy kalkulacyjnych raporty dostępne do oglądania przez przeglądarkę Internetową bez zainstalowanych innych narzędzi klienckich.    14. Możliwość automatyzacji usuwania duplikatów dokumentów. 8. Wyszukiwanie treści:    1. Pełnotekstowe indeksowanie zawartości intranetu w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez webservice.    2. Centralny mechanizm wyszukiwania treści dostępny dla użytkowników intranetu.    3. Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, oraz zakresów dat publikacji.    4. Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów intranetu wg zadanych kryteriów, np. wg typów dokumentów.    5. Możliwość definiowania słownika słów wykluczonych (często używanych).    6. Możliwość tworzenia „linków sponsorowanych”, prezentowanych wysoko w wynikach wyszukiwania w zależności od słów wpisanych w zapytaniu.    7. Podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu.    8. Przedstawianie w wynikach duplikatów plików.    9. Statystyki wyszukiwanych fraz. 9. Administracja intranetem i inne funkcje:    1. Możliwość definiowania ról / grup uprawnień, w ramach których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami dostępna dla administratorów merytorycznych intranetu, niewymagająca szczególnych kompetencji technicznych.    2. Możliwość określania uprawnień do poszczególnych elementów zawartości intranetu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu.    3. Generowanie powiadomień pocztą elektroniczną dla użytkowników intranetu z informacją o publikacji najbardziej istotnych treści.    4. Definiowanie metryk opisujących dokumenty w poszczególnych repozytoriach portalu oraz centralnie zarządzanego zbioru metadanych z wyznaczonym administratorem merytorycznym.    5. Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i webservice oraz wykorzystywania ich do opisywania dokumentów.    6. Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów intranetu.    7. Statystyki odwiedzin poszczególnych części i stron intranetu – analiza liczby odsłon w czasie. Opcjonalnie zaawansowane statystyki i analizy.    8. Funkcjonalności wspierające pracę grupową - do wykorzystania na najniższym poziomie intranetu do celów pracy działów i zespołów zadaniowych. Funkcjonalności wspierające gromadzenie dokumentów, wsparcie komunikacji, planowanie zadań i wydarzeń    9. Funkcjonalność publikowania na portalu formularzy elektronicznych XML i przetwarzanych na aplikację webową dostępną dla użytkowników przez przeglądarkę Internetową. Dane z wypełnionego formularza mają być zapisywane w formacie XML zgodnie z definicją formularza.    10. Mechanizmy wspierające przepływy pracy (workflow) wraz z funkcjonalnością definiowania procesów obiegu dokumentów, integracji przepływów z web-services, wywoływania web-services z poziomu workwlow bez konieczności kodowania przy wykorzystaniu prostych w obsłudze narzędzi portalu. |

**4.7. System uprawnień**

Dostawa, wdrożenie i utrzymanie usługi systemu uprawnień (Microsoft Active Directory lub równoważny) dla każdego użytkownika końcowego Zamawiającego w ramach Usługi podstawowej i Usług dodatkowych.

Tabela nr 10. Tabela równoważności.

|  |  |
| --- | --- |
| Microsoft Active Directory | 1. System równoważny do Active Directory musi spełniać następujące wymagania:    1. umożliwia scentralizowane zarządzanie obiektami (serwery, drukarki czy udostępnione pliki), a także przypisywanie uprawnień do tychże zasobów,    2. umożliwiająca uwierzytelnienie obiektów (np. użytkowników, komputerów) i autoryzacja (lub jej odmowa) dostępu do innych obiektów (dowolnych, np. kontenera lub obiektu użytkownika) oraz do zasobów innych, w tym dyskowych, sieciowych oraz aplikacji,    3. umożliwia konfigurację obiektów,    4. możliwość działania w rozproszonych sieciach,    5. możliwość działania w środowisku Microsoft Windows Server,    6. możliwość konfiguracji za pomocą narzędzi graficznych i z linii komend,    7. możliwość tworzenia skryptów,    8. aktywne wsparcie protokołu LDAP (Lightweight Directory Access Protocol). 2. Obiekty:    1. Konto użytkownika – obiekt zawierający informacje o użytkowniku,    2. Kontakt – obiekt zawierający informacje kontaktowe użytkowników,    3. Komputer – obiekt zawierający informacje o komputerze,    4. Drukarka – obiekt zawierający odniesienie (wskaźnik) do drukarek sieciowych,    5. Udział sieciowy – obiekt zawierający odniesienie do udostępnionych folderów w sieci,    6. Grupa – obiekt zawierający kolekcję innych obiektów, stosowany do zarządzania uprawnieniami,    7. Jednostka organizacyjna – obiekt administracyjny obejmujący inne obiekty, stasowany do zarządzania konfiguracją,    8. Domena – podstawowa struktura systemu, w ramach której zdefiniowane są pozostałe obiekty,    9. Kontroler Domeny – obiekt zawierający informację o serwerze pełniącym funkcję kontrolera domeny,    10. Lokalizacja (Site) – obiekt zawierający informację o podsieciach w danej lokalizacji,    11. Builtin – grupy o predefiniowanych uprawnieniach do wykonywania czynności administracyjnych,    12. Relacja zaufania – obiekt zawierający informację o relacjach zaufania pomiędzy domenami. |

**4.8. Podłączenie do serwera OCS**

Podłączenie każdego użytkownika końcowego Zamawiającego w ramach Usługi podstawowej i Usług dodatkowych do serwera OCS.

**4.9. Łącza internetowe**

1. Łącza do sieci publicznej (Internet)

Przepustowość symetrycznego łącza, zapewnionego w ramach realizacji Usługi, musi być nie mniejsza niż 100 Mbit/s z możliwością zwiększenia na żądanie Zamawiającego. Łącze musi posiadać ochronę przed atakami DDoS.

1. Łącze światłowodowe dedykowane

Wykonawca zapewni dedykowane łącze do siedziby Zamawiającego wraz z niezbędnymi urządzeniami aktywnymi. Przesyłanie danych będzie odbywać się poza siecią publiczną. Przepustowość łącza dedykowanego będzie wynosić min. 1 Gbps z możliwością zwiększenia na żądanie Zamawiającego.

1. **Usługa dodatkowa.**

Usługa dodatkowa maja charakter Prawa Opcji. Oznacza to, że Zamawiający ma prawo złożyć zamówienie na te usługi lecz nie ma takiego obowiązku. W przypadku nie skorzystania przez Zamawiającego z usług dodatkowych Wykonawcy nie będzie przysługiwało roszczenie o ich wykonanie jaki żadne roszczenie finansowe. W przypadku skorzystania z usług dodatkowych Wykonawca otrzyma wynagrodzenie odpowiadające iloczynowi ceny jednostkowej określonej w Ofercie dla danej usługi i liczby usług faktycznie zrealizowanych.

5.1. Poczta email zgodnie z parametrami w pkt. 4.4. SIWZ - maksymalnie dodatkowo 40 nowych kont pocztowych.

5.2. Ochrona antywirusowa zgodnie z parametrami w pkt. 4.5. SIWZ – maksymalnie dodatkowo 40 nowych stacji roboczych.

5.3. Usługa katalogowa zgodnie z parametrami w pkt. 4.6. SIWZ – maksymalnie dodatkowo 40 nowych użytkowników.

5.4. Usługa wynajmu komputera przenośnego (laptop) o parametrach w tabeli poniżej – maksymalnie 10 komputerów przenośnych.

Tabela nr 11. Minimalne wymagania dot. komputerów przenośnych.

|  |  |
| --- | --- |
|  | Minimalne wymagania Zamawiającego |
| a | Procesor minimum dwu rdzeniowy, minimum 2 GHz; |
| b | Pamięć RAM minimum 4 GB;  Dysk twardy o pojemności min. 500 GB; |
| d | System operacyjny Windows 10 Professional lub równoważny |
| e | Microsoft Office 365 lub równoważny |
| f | Oprogramowanie antywirusowe |

1. **Zamówienia podobne na podstawie art. 67 ust. 1 pkt 6 ustawy pzp.**

Zamawiający przewiduje udzielanie zamówienia, o którym mowa w art. 67 ust. 1 pkt 6 ustawy pzp. Zamawiający przewiduje możliwość udzielenia wybranemu wykonawcy zamówienia podobnego do 50% wartości zamówienia podstawowego (usługa podstawowa +usługa dodatkowa). Zamówienie może być udzielone w terminie 3 lat od zawarcia umowy o zamówienie podstawowe. Przedmiotem zamówienia uzupełniającego mogą być wszystkie usługi będące przedmiotem zamówienia podstawowego lub tylko niektóre z nich, z możliwością zmian ilości, realizowane w zakresie i na warunkach zamówienia podstawowego. Umowa o zamówienie podobne będzie udzielona na warunkach określonych we wzorze umowy dla zamówienia podstawowego.

1. **Obowiązek zatrudnienia na umowę o pracę osób**

Zamawiający wymaga zatrudnienia przez Wykonawcę, jak i podwykonawcę, na podstawie umowy o pracę osób wykonujących w zakresie realizacji zamówienia czynności polegające na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (t.j. Dz.U. z 2018r. poz. 917 z późń. zm.), tj. osób wykonujących następujące czynności:

1. opracowywanie założeń i architektury systemów informatycznych,
2. administrowanie urządzeniami sieciowymi,
3. administrowanie serwerami w środowisku wirtualnym,
4. administrowanie systemami operacyjnymi.

Sposób dokumentowania zatrudniania osób, o których mowa powyżej, uprawnienia Zamawiającego w zakresie kontroli spełniania przez Wykonawcę wymagań z tytułu zatrudnienia na podstawie umowy o pracę oraz sankcje z tytułu niespełnienia tych wymagań zostały określone w załączniku do SIWZ - “Wzór umowy”.