**Załącznik nr 1**

**Szczegółowy opis przedmiotu zamówienia**

czerwiec 2022

Spis treści

[1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego. 3](#_Toc103853031)

[2. Wymagania gwarancyjne. 3](#_Toc103853032)

[3. Miejsce instalacji sprzętu i oprogramowania/systemu. 3](#_Toc103853033)

[4. Ubezpieczenie sprzętu 4](#_Toc103853034)

[5. Zestawienie zakresu dostaw i usług. 4](#_Toc103853035)

[5.1. Stacje robocze – szt. 4 – wymagania minimalne 6](#_Toc103853036)

[5.2. Serwer NAS do backupu – zdalne repozytorium – szt. 1 – wymagania minimalne 14](#_Toc103853037)

[5.3. Urządzenia do zabezpieczenie poczty internetowej – szt. 1 – wymagania minimalne 15](#_Toc103853038)

[5.4. Przedłużenie wsparcia dla urządzenia firewall - szt. 1 – wymagania minimalne 18](#_Toc103853039)

[5.5. Przedłużenie wsparcia dla oprogramowania do wirtualizacji – szt. 1 – wymagania minimalne 18](#_Toc103853040)

[5.6. Przedłużenie wsparcia dla oprogramowania do backupu.– szt. 1 – wymagania minimalne 19](#_Toc103853041)

[5.7. Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania – Przegląd urządzenia UPS 23](#_Toc103853042)

[5.8. Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania – instalacja i konfiguracja 24](#_Toc103853043)

[5.9. Diagnoza cyberbezpieczeństwa 26](#_Toc103853044)

## Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

* całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
* całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

## Wymagania gwarancyjne.

**Sprzęt**

* o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. roczna gwarancja (chyba, że zapisy szczegółowe stanowią inaczej) oparta na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
* Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
* Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
* Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;
* wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń sieciowych i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

## Miejsce instalacji sprzętu i oprogramowania/systemu.

* Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części załącznika na 1, w budynkach urzędu w miejscach wskazanych przez Zamawiającego.

## Ubezpieczenie sprzętu

Wykonawca zobowiązany jest do dostawy sprzętu komputerowego wraz z ubezpieczeniem na okres 12 m-cy. Koszty ubezpieczenia należy ująć w cenie oferowanego sprzętu.

Sprzęt musi zostać ubezpieczony do 100% jego wartości księgowej brutto.

Ubezpieczenie nie może przewidywać franszyzy, integralnej i udziału własnego ze strony Zamawiającego.

Polisa ubezpieczeniowa powinna zostać wystawiona na rzecz Zamawiającego.

Dostarczony sprzęt powinien zostać objęty ubezpieczeniem od wszelkich ryzyk zgodnie z poniższymi założeniami:

1. Przedmiotem ubezpieczenia jest sprzęt elektroniczny stacjonarny zainstalowany na stałe w

miejscu ubezpieczenia oraz sprzęt przenośny, pod warunkiem, że wiek sprzętu elektronicznego stacjonarnego i sprzętu przenośnego nie przekracza 5 lat.

1. Sprzęt przenośny używany poza lokalem na terenie Rzeczypospolitej Polskiej jest objęty ochroną w przypadku jego utraty wskutek kradzieży z włamaniem, jeżeli został skradziony z samochodu, gdy:
   1. pojazd posiadał twardy dach (jednolitą sztywną konstrukcję),
   2. został prawidłowo zamknięty na wszystkie możliwe zabezpieczenia znajdujące się w pojeździe,
   3. był zaparkowany w zamkniętym garażu lub na parkingu strzeżonym (jeżeli kradzież z włamaniem nastąpiła w godzinach 22.00 - 6.00),
   4. ubezpieczony przedmiot był przechowywany wewnątrz pojazdu w sposób uniemożliwiający zobaczenie go z zewnątrz, np. w bagażniku.
2. Zakres ubezpieczenia:
3. Od wszystkich ryzyk z rozszerzeniem o użytkowanie mobilne w tym m.in.:
   1. utrata bądź ubytek wartości ubezpieczonego sprzętu nastąpiły z powodu jego zniszczenia lub uszkodzenia w wyniku nieprzewidzianego wypadku uniemożliwiającego dalsze spełnianie zamierzonych funkcji.
   2. utrata sprzętu nastąpiła wskutek kradzieży z włamaniem, rabunku, dewastacji i wandalizmu.
4. Do szkód objętych ubezpieczeniem zalicza się m.in. szkody wynikłe w następstwie:
5. działania człowieka:
   1. niewłaściwej obsługi sprzętu, tj. nieostrożności, zaniedbania, niewłaściwego użytkowania,
   2. braku kwalifikacji, błędu operatora itp.;
   3. świadomego i celowego zniszczenia przez osoby trzecie, pracowników i współpracowników ubezpieczającego (jednak z zastosowaniem klauzuli reprezentantów),
6. kradzieży z włamaniem, rabunku, wandalizmu i dewastacji. Ubezpieczyciel ponosi odpowiedzialność także za szkody powstałe wskutek kradzieży z pojazdu lub kradzieży całego pojazdu wraz ze sprzętem.
7. ognia (w tym działania dymu, sadzy itp.) oraz polegające na osmaleniu, przypaleniu, a także w wyniku wszelkiego rodzaju eksplozji, implozji, uderzenia piorunu bezpośrednio i pośrednio na przedmiot ubezpieczenia, upadku statku powietrznego oraz w akcji ratunkowej
8. wody, tj. zalania wodą z urządzeń wodno – kanalizacyjnych, powodzi, wylewu wód podziemnych, a także czynników atmosferycznych w postaci mrozu, śniegu, deszczu wilgoci, pary wodnej itp.
9. wiatru, gradu, lawiny, obsunięcia i zapadania się ziemi, huraganu, trzęsienia ziemi,
10. zbyt wysokiego lub zbyt niskiego napięcia albo całkowitego zaniku napięcia w sieci instalacji elektrycznej, szkód przepięciowych i pochodnych powstałych w związku z uderzeniem pioruna,
11. sprzęt elektroniczny ubezpieczony jest również w zakresie szkód spowodowanych przez upadek.
12. Dodatkowe rozszerzenie dotyczące ochrony sprzętu nie podłączonego na stanowisku pracy lub podczas przerwy w eksploatacji.

## Zestawienie zakresu dostaw i usług.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa** | **Długość gwarancji (minimum) [m-ce]** | **Ilość** | **Jednostka miary** | **Uwagi** |
|  | Stacje robocze | 12 (kryterium oceny) | 4 | Szt. | Pozycja dotyczy zakupu komputerów z oprogramowaniem do pracy biurowej. Typ AIO; 24 cale, 8 Gb RAM, 256 SSD, system operacyjny, oprogramowanie biurowe. |
|  | Serwer NAS do backupu – zdalne repozytorium | 12 (kryterium oceny) | 1 | Szt. | Pozycja dotyczy zakupu serwera NAS (backupu) jako miejsca przechowywania kopii bezpieczeństwa. Serwer zostanie zlokalizowany w zdalnej, drugiej serwerowni – w drugim budynku urzędy. Min. 4 dyski 6 TB. |
|  | Urządzenia do zabezpieczenie poczty internetowej. | 12 (kryterium oceny) | 1 | Szt. | Pozycja dotyczy zakupu dedykowanego urządzenia (maszyna wirtualna lub urządzenie fizyczne) do zabezpieczenia wewnętrznego serwera pocztowego, zapewniającego między innymi filtrację i ochronę ruchu w zakresie skanowania antywirusowego i antyspamowego. Dodatkowo pozwoli na bezpieczną publikację usług serwera pocztowego z możliwością oferowania pracy zdalnej – bezpiecznego dostępu z wykorzystanie połączeń VPN na publicznej sieci Internet. |
|  | Przedłużenie wsparcia dla urządzenia firewall | 12 (kryterium oceny) | 1 | Szt. | Pozycja dotyczy zakupu wsparcia dla posiadanego przez Gminę firewall’a firmy Fortinet model FG-101-E. Wykupione wsparcie pozwoli na zapewnieni dostępu do najnowszych wersji oprogramowania co zdecydowanie wpłynie na bezpieczeństwo pracy jak i świadczonych usług. |
|  | Przedłużenie wsparcia dla oprogramowania do wirtualizacji. | 12 (kryterium oceny) | 1 | Szt. | Pozycja dotyczy wykupienia przedłużenia licencji serwisów wsparcia dla posiadanego oprogramowania do wirtualizacji - VMware vSphere 6 Essentials Plus. Wykupione wsparcie pozwoli na zapewnienia dostępu do najnowszych wersji oprogramowani i jego aktualizacji co zdecydowanie wpłynie na bezpieczeństwo pracy jak i świadczonych usług. Zakup jednorazowy |
|  | Przedłużenie wsparcia dla oprogramowania do backupu. | 12 (kryterium oceny) | 1 | Szt. | Pozycja dotyczy wykupienia przedłużenia licencji serwisów wsparcia dla posiadanego oprogramowania do backupu i archiwizacji danych - Veeam Backup Essentials. Wykupione wsparcie pozwoli na zapewnieni dostępu do najnowszych wersji oprogramowania i jego aktualizacji co zdecydowanie wpłynie na bezpieczeństwo pracy jak i świadczonych usług. Zakup jednorazowy. |
|  | Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania  UPS (20kV) - serwis (przegląd urządzenia) | Nd. | 1 | Szt. | Pozycja dotyczy kosztu wykonania usługi przeglądu serwisowego dla urządzenia UPS, które podtrzymuje zasilanie dla całej serwerowni. Zakup konieczny do zapewnienie odpowiednich warunków pracy dla urządzeń serwerowych. |
|  | Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania  Instalacja i konfiguracja | 12 | 1 | Szt. | Usługi obejmować będą: a) Aktualizację oprogramowania układowego serwerów, macierzy, firewall. b) Opracowanie polityk bezpieczeństwa sieci, wymiany danych. c) Aktualizację oprogramowania do wirtualizacji i backupu. d) Instruktaż dla służb informatycznych. e) Wsparcie techniczne, nadzór autorski 12 miesięcy. Łącznie przewidziano 25 godz. roboczych |
|  | Diagnoza cyberbezpieczeństwa | 12 | 1 | Szt. | Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina". |

## Stacje robocze – szt. 4 – wymagania minimalne

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
|  | Zastosowanie | Komputer All in One, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
|  | Matryca | - Zintegrowana w jednej obudowie z PC  - Typ ekranu: 23.5-24”  - Jasność: min. 250 cd/m2  - Kontrast: min. 1000:1  - Kąty widzenia (pion/poziom): min. 178°/178°  - Czas reakcji matrycy: maks. 14 ms  - Kolory: min. 16.7mln  - Obsługiwana rozdzielczość: min. 1920 x 1080  - Powłoka powierzchni ekranu: Przeciwodblaskowa  - Zakres pochylenia względem podstawy: w nie mniejszy niż 0°-20°  - Regulacja wysokości: min. 130 mm |
|  | Wydajność | Procesor klasy x86 ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach biurowych, osiągający w teście wydajności (BAPCO):  Sysmark 2018 – Overall Rating wynik min.1300  Productivity – co najmniej wynik 1300 punktów  Creativity – co najmniej wynik 1300 punktów  Responsiveness – co najmniej wynik 1300 punktów  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta. |
|  | Pamięć RAM | Pamięć operacyjna: 8GB 2933 możliwość rozbudowy do min 64 GB. Jeden slot wolny. |
|  | Pamięć masowa | Dysk SSD PCIe M.2 NVMe o pojemności min. 256 GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników, wspierający technologię sprzętowego szyfrowania danych. |
|  | Zintegrowana karta graficzna | Wydajność grafiki: Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Obsługująca funkcje: DirectX 12, OpenGL 4.5. |
|  | Sieć | Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika) |
|  | Bezpieczeństwo | Złącze umożliwiające zabezpieczenie komputera przed wyniesieniem,  Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Co najmniej TPM 2.0.  Certyfikowane oprogramowanie producenta komputera umożliwiające – bez względu na stan czy obecność systemu operacyjnego w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego. |
|  | Multimedia | Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition audio. Głośniki stereo.  Porty audio wymagane zarówno na przednim, jak i na tylnym panelu obudowy. Kamera FHD chowana w obudowie. Wewnętrzny mikrofon stereo. |
|  | Zasilanie | Wewnętrzny zasilacz o mocy minimum 190 W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 93%, przy obciążeniu 50%. |
|  | Wymiary | Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych bez stopy monitora) nie może wynosić więcej niż 1000mm. |
|  | Obudowa | Zintegrowana z monitorem (AiO), wyposażona w min. 2 kieszenie: 1 szt. 5,25” zewnętrznie (dopuszcza się zatokę na napęd optyczny typu SLIM), 1 szt. 2,5” wewnętrzne.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki).  Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością demontażu stopy. Stopa dostarczona w zestawie.  Obudowa trwale oznaczona logiem producenta. |
|  | BIOS | Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:  - modelu komputera;  - modelu płyty głównej;  - nr seryjnego komputera;  - wersji BIOS (z datą);  - modelu procesora wraz z informacjami o prędkości taktowania;  - Informacji o ilości i obsadzeniu slotów pamięci RAM wraz z informacją o prędkości taktowania;  - Informacji o dysku twardym: model oraz pojemność  - MAC adresie zintegrowanej karty sieciowej  - temperaturze układu graficznego  - temperaturze procesora  - temperaturze wewnątrz obudowy komputera  - statusu karty sieciowej |
|  | System operacyjny | Zainstalowany system operacyjny spełniający następujące wymagania techniczne:   * dostępne dwa rodzaje graficznego interfejsu użytkownika, w tym:   + klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,   + dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych; * interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim; * możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; * możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; * darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; * internetowa aktualizacja zapewniona w języku polskim; * wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; * zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; * wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); * funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer; * 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; * możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; * zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; * 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; * zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; * funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego; * funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika; * zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi; * wbudowany system pomocy w języku polskim; * możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); * możliwość zarządzania stacją roboczą poprzez polityki – przez politykę należy rozumieć zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; * wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; * automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; * wsparcie dla logowania przy pomocy smartcard; * rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; * system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; * wsparcie dla Java i .NET Framework 1.1 i 2.0 i 3.0 – 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 ma umożliwiać 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; * udostępnianie modemu; * 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 min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.); * możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). |
|  | Inne | Zainstalowany pakiet biurowy spełniający następujące wymagania techniczne:   * 1. wymagania odnośnie interfejsu użytkownika: * pełna polska wersja językowa interfejsu użytkownika, * prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych;   1. oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: * posiada kompletny i publicznie dostępny opis formatu, * 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 (Dz. U. 2012, poz. 526);   1. oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji;   2. w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy);   3. do aplikacji musi być dostępna pełna dokumentacja w języku polskim;   Pakiet zintegrowanych aplikacji biurowych musi zawierać:   1. Edytor tekstów, 2. Arkusz kalkulacyjny, 3. Narzędzie do przygotowywania i prowadzenia prezentacji, 4. Narzędzie do tworzenia drukowanych materiałów informacyjnych, 5. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), 6. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR;   Edytor tekstów musi umożliwiać:   * edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, * wstawianie oraz formatowanie tabel, * wstawianie oraz formatowanie obiektów graficznych, * wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), * automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, * automatyczne tworzenie spisów treści, * formatowanie nagłówków i stopek stron, * śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, * nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, * określenie układu strony (pionowa/pozioma), * wydruk dokumentów, * wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, * pracę na dokumentach utworzonych przy pomocy posiadanego przez Zamawiającego oprogramowania Microsoft Word 2003 lub Microsoft Word 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, * zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, * wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem, * wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa;   Arkusz kalkulacyjny musi umożliwiać:   * tworzenie raportów tabelarycznych, * tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, * tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, * tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService), * obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, * tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, * wyszukiwanie i zamianę danych, * wykonywanie analiz danych przy użyciu formatowania warunkowego, * nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, * nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, * formatowanie czasu, daty i wartości finansowych z polskim formatem, * zapis wielu arkuszy kalkulacyjnych w jednym pliku, * zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, * zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;   Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:   * przygotowywanie prezentacji multimedialnych, * prezentowanie przy użyciu projektora multimedialnego, * drukowanie w formacie umożliwiającym robienie notatek, * zapisanie jako prezentacja tylko do odczytu, * nagrywanie narracji i dołączanie jej do prezentacji, * opatrywanie slajdów notatkami dla prezentera, * umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, * umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, * odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, * możliwość tworzenia animacji obiektów i całych slajdów, * prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, * pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint   Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:   * tworzenie i edycję drukowanych materiałów informacyjnych, * tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów, * edycję poszczególnych stron materiałów, * podział treści na kolumny, * umieszczanie elementów graficznych, * wykorzystanie mechanizmu korespondencji seryjnej, * płynne przesuwanie elementów po całej stronie publikacji, * eksport publikacji do formatu PDF oraz TIFF, * wydruk publikacji, * możliwość przygotowywania materiałów do wydruku w standardzie CMYK;   Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:   * pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, * przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, * filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, * tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, * automatyczne grupowanie poczty o tym samym tytule, * tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, * oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, * mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, * zarządzanie kalendarzem, * udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, * przeglądanie kalendarza innych użytkowników, * zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, * zarządzanie listą zadań, * zlecanie zadań innym użytkownikom, * zarządzanie listą kontaktów, p) udostępnianie listy kontaktów innym użytkownikom, * przeglądanie listy kontaktów innych użytkowników, * możliwość przesyłania kontaktów innym użytkowników. |
|  | Normy i standardy | Komputery mają spełniać normy i posiadać deklaracje zgodności w zakresie:  -Deklaracja zgodności CE (lub równoważne np.: EPAT)  Certyfikaty te mają na celu wykazanie, iż producent na etapie wytworzenia produktu podjął się spełnienia wyższych wymagań ze względu na aspekty środowiskowe, zdrowotne i ergonomie, a tym między innymi dotyczące:  1. Wydajności energetycznej  2. Bezpieczeństwa promieniowania i emisji elektromagnetycznej (testowanie produktów pod względem bezpieczeństwa podzespołów elektrycznych i emisji elektro-magnetycznej)  3. Żywotności produktu (wydłużone normy czasowe dla bezawaryjnej pracy)  4. Systemu zarządzania środowiskiem  5. Odpowiedzialności społecznej za warunki pracy (programy CSR – Corporate Social Responsibility Społecznej Odpowiedzialność biznesu – włączając EICC (wspieranie praw pracowniczych) i SA8000 (lub równoważne) – standardu certyfikacji opierający się na normach dotyczących praw człowieka, audyt warunków pracy)  6. Zmniejszenia występowania niebezpiecznych substancji (kadm, rtęć, ołów i chrom sześciowartościowy)  7. Designu oraz recyclingu (bezpieczeństwa utylizacji produktu)  8. Ergonomiki i przystosowania produktu przyjaznego w użytkowaniu (kąty widzenia, ostrość i kontrast, właściwości akustyczne).  -Być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001 (lub równoważne)  -Posiadać certyfikat TCO Certified All-in-One PC 8 (lub równoważne)  -Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 w pozycji operatora w trybie jałowym (IDLE) wynosząca maksymalnie 18 dB(A) (lub równoważne) |
|  | Porty i złącza | - 1 x Display Port  - 1 x Audio: line-in - 1 x Audio: line-out - 1 x Audio: słuchawki z przodu obudowy  - 1 x RJ45 (karta sieciowa)  - 7 szt. USB w tym: minimum 3 porty z przodu obudowy (w tym min. 2x USB 3.2 gen1 typ A oraz min. 1x USB 3.2 gen1 typ C ), minimum 4 porty z tyłu obudowy (w tym min. 1x USB 3.2 gen1 typ A). Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.  Płyta główna:  - minimum dwa złącza pamięci RAM z obsługą do 64 GB pamięci  - min. 2 złącza SATA 3.0 (6 Gbit) NCQ,  - co najmniej jedno złącze M.2-2280 (SSD NVMe),  - co najmniej jedno złącze M.2-2230 (WLAN). |
|  | Klawiatura | Klawiatura USB w układzie polski programisty, 104 klawisze – trwale oznaczona logo producenta jednostki centralnej |
|  | Mysz | Mysz optyczna USB z trzema klawiszami oraz rolką (scroll) – trwale oznaczona logo producenta jednostki centralnej |
|  | Gwarancja | Gwarancja jakości producenta świadczona 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,   * + Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta oferowanego komputera   + Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela   Zgłoszenia serwisowe w języku polskim:   * Na dedykowaną infolinie producenta komputera oraz na dedykowany adres email. * Poprzez formularz zgłoszeniowy online dostępny na stronie producenta komputera |

## Serwer NAS do backupu – zdalne repozytorium – szt. 1 – wymagania minimalne

|  |
| --- |
| * Procesor osiągający w teściem CPU Mark na stronie <https://www.cpubenchmark.net/cpu_list.php> wartość min. 5200 punktów * Prędkość odczytu, min. 450.00 MB/sek * Prędkość zapisu min. 450.00 MB/sek * Wbudowany interfejs 1Gbit/s z min. czterema portami RJ-45 oraz funkcją agregacji łączy * Możliwość zainstalowania karty SSD M.2 lub 10GbE * Pamięć RAM min. 4GB (możliwość rozbudowy do min. 32 GB w min 2 slotach) * Ilość kieszeni dysków min. 8 (możliwość rozbudowy do 12 dysków z wykorzystaniem jednostki rozszerzającej lub równoważnie obudowa na 12 dysków) * Obudowa 19 cali max. 2U z szynami do montaży w szafie teleinformatycznej * Port USB 3.0 min. 2 szt. * Port eSATA min 1 szt. * Obsługiwane typy dysków:   + 3,5” SATA HDD   + 2,5” SATA HDD   + 2,5” SATA SSD * Obsługiwany poziom RAID:   + Basic   + JBOD   + [RAID 0](https://www.komputronik.pl/search-filter/7071/serwer-nas-z-raid-0)   + RAID 1   + RAID 10   + [RAID 5](https://www.komputronik.pl/search-filter/7071/serwer-nas-z-raid-5)   + RAID 6 * Urządzenie musi zostać dostarczone z min. 4 szt. dysków twardych o pojemności min 6TB. * Wsparcie dla środowisk wirtualizacji takich jak VMware, Citrix oraz Microsoft Hyper-V. * Wbudowany serwer FTP z funkcjami SSL, TLS. * Obsługa Windows AD, LDAP oraz Domain Trust. * Ochrona za pomocą funkcji kopii zapasowych, jednostek LUN, migawek, klonowania i synchronizacji danych. * Panel użytkownika i oprogramowanie dostępne w pełnej polskiej wersji językowej. * Wbudowane systemy zabezpieczeń sieciowych, antywirus, szyfrowanie AES256bit oraz dwustopniowe uwierzytelnianie użytkowników. * Urządzenie musi być wyposażone w zintegrowane rozwiązanie do tworzenia kopii zapasowych dla serwerów fizycznych z systemem Windows/Linus, komputerów z systemem Windows, serwerów plików rsync/SMB oraz maszyn wirtualnych VMware vSphere/Microsoft Hyper-V. * Urządzenie musi posiadać centralny interfejs zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, zużycia pamięci masowej i transmisji danych historycznych. * Oprogramowanie do backupu musi umożliwiać szybkie przywracanie plików, całych maszyn fizycznych i maszyn wirtualnych. |

## Urządzenia do zabezpieczenie poczty internetowej – szt. 1 – wymagania minimalne

|  |
| --- |
| Wymagania ogólne  System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.  Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.  Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:   1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).   Parametry fizyczne systemu antyspamowego   1. System musi być wyposażony w interfejsy:  * 4 porty Gigabit Ethernet RJ-45.  1. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB . 2. System musi posiadać wbudowany port konsoli szeregowej. 3. Zasilanie z sieci 230V/50Hz.   Ogólne funkcje systemu ochrony poczty  Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:   1. Wsparcie dla co najmniej 20 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys. wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, antyspam, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail lub IMAP. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.   Kontrola antywirusowa i ochrona przed malware  W tym zakresie dostarczony system ochrony poczty musi zapewniać:   1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 9. Ochronę typu wirus outbrake.   Kontrola antyspamowa  System musi zapewniać poniższe funkcje i metody filtrowania spamu:   1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej. 13. Ochrona typu outbrake. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.   Ochrona przed atakami na usługę poczty  System musi zapewniać poniższe funkcje i metody filtrowania:   1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing). 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy.   Funkcje logowania i raportowania  W tym zakresie dostarczony system ochrony poczty musi zapewniać:   1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.   Funkcje pracy w trybie wysokiej dostępności (HA)  System ochrony poczty musi zapewniać poniższe funkcje:   1. Konfigurację HA w każdym z trybów: gateway, transparent. 2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowanie stanu pracy klastra.   Aktualizacje sygnatur, dostęp do bazy spamu  W tym zakresie dostarczony system ochrony poczty musi zapewniać:   1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.   Zarządzanie  System ochrony poczty musi zapewniać poniższe funkcje:   1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.   Certyfikaty  Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:   1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.   Serwisy i licencje  W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:   1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake.   Gwarancja oraz wsparcie   1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.   Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 / 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5 / 24x7. |

## Przedłużenie wsparcia dla urządzenia firewall - szt. 1 – wymagania minimalne

|  |
| --- |
| Zamawiający oczekuje przedłużenia wsparcia dla posiadanego urządzeń firewall firmy Fortinet model 101E o numerze seryjnym: FG101E4Q17002533  Pozycja dotyczy zakupu 1 szt.:  FC-10-F101E-950-02-DD Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare). |

## Przedłużenie wsparcia dla oprogramowania do wirtualizacji – szt. 1 – wymagania minimalne

|  |
| --- |
| Zamawiający oczekuje przedłużenia wsparcia dla posiadanego oprogramowania do wirtualizacji firmy Vmware o numerze kontraktu - Contract ID: 465458712  Pozycja dotyczy zakupu:  VS6-ESP-KIT-G-SSS-C - Basic Support Coverage  VMware vSphere 6 Essentials Plus Kit for 3 hosts (Max 2 processors per host)  Lub równowaznie:  Licencja dla 3 serwerów fizycznych posiadających 2 procesory ze wsparciem technicznym 9x5 z 4h-czasem zdalnej reakcji oraz gwarancją utrzymania aktualnej wersji przez okres min. 1 rok.  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. |

## Przedłużenie wsparcia dla oprogramowania do backupu.– szt. 1 – wymagania minimalne

|  |
| --- |
| Zamawiający oczekuje przedłużenia wsparcia dla posiadanego oprogramowania do backupu firmy Veeam - Backup Essentials Enterprise 2 socket bundle. (Support ID=01015258)  lub równoważnie:    **Wymagania ogólne**  Minimalna ilość licencji musi umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 30 VM oraz 4 serwerów fizycznych.  Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej  Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.  Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.  Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.  **Całkowite koszty posiadania**  Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej  Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków  Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)  Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji  Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.  Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.  Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania  Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.  Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)  Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji  Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji  Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania  Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)  Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.  **Wymagania RPO**  Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej  Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.  Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych  Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora  Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.  Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn  Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)  Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.  Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.  Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.  Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)  Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.  Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik  Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)  Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)  **Wymagania RTO**  Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.  Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)  Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami  Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre  Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków  Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.  Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików  Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.  Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:  o Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs  o BSD: UFS, UFS2  o Solaris: ZFS, UFS  o Mac: HFS, HFS+  o Windows: NTFS, FAT, FAT32, ReFS  o Novell OES: NSS  Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.  Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.  Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.  Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.  Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),  Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska  Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych  Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska  Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych  Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.  Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.  Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego  Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN  **Ograniczenie ryzyka**  Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.  Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem  Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere  Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.  Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.  **Monitoring**  System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich  System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie  System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.  System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware  System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter  System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn  System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel  System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk  System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora  System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów  System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)  System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna  System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego  System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta  System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.  System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.  System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware  System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x  **Raportowanie**  System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022  System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.  System musi być certyfikowany przez VMware i posiadać status „VMware Ready”  System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V  System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF  System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc  System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach  System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów  System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych  System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych  System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury  System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta  System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.  System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.  System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware  System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)  System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |

## Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania – Przegląd urządzenia UPS

|  |
| --- |
| Zamawiający wymaga przeprowadzenia przeglądu okresowego dla posiadanego urządzenia UPS.  Model NGS 20 o numerze seryjnym I01169017641. |

## Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania – instalacja i konfiguracja

|  |  |  |
| --- | --- | --- |
| Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania. | | |
|  | **Usługi** | Celem prac jest przygotowanie odnowienie środowiska teleinformatycznego, na potrzeby realizacji e-usług publicznych, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.  Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego.  Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. |
|  | **Montaż i fizyczne uruchomienie systemu** | **Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:**   1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. 2. Rozbudowa istniejących zasobów sprzętowych. 3. Urządzenia, które nie są montowane w szafach teleinformatycznych np.: komputery, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 6. Wykonanie procedury aktualizacji firmware dostarczonych i posiadanych elementów sprzętowych (serwer, macierz, firewall, przełączniki sieci LAN) do najnowszej wersji oferowanej przez producenta sprzętu. 7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). |
|  | **Aktualizacja i konfiguracja oprogramowania** | 1. Aktualizacja (podniesienie wersji do najnowszej możliwej wynikającej z zaoferowanego wsparcia) i/lub konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z migracją odpowiedniej liczby wirtualnych maszyn na potrzeby rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. 2. Aktualizacja (podniesienie wersji do najnowszej możliwej wynikającej z zaoferowanego wsparcia) i konfiguracja dostarczonego oprogramowania do systemu wykonywania backupu i archiwizacji danych. 3. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia dla następujących istniejących urządzeń:    1. Serwer - Fujitsu 4 szt. PY RX2540 M4    2. Macierz dyskowa – 1 szt. Fujitsu DX200S4    3. Klaster firewall FG-101F    4. Przełączników sieci LAN – Cisco – 42 szt. C2960 |
|  | **Dołączenie stacji roboczych do domeny** | Zamawiający wymaga dołączenia wszystkich dostarczonych stacji roboczych do domeny. W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mająca na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (miedzy innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na konto domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji). |
|  | **Testowanie i modyfikacja parametrów infrastruktury sieciowej.** | Po przeprowadzonych aktualizacjach należy przeprowadzić:   1. Testowanie mechanizmów bezpieczeństwa serwera. 2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. 3. Testowanie dostępu publicznego do zasobów. 4. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu 5. Testowanie autoryzowanego dostępu do wewnętrznych zasobów. 6. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach |
|  | **Szkolenie – instruktaż stanowiskowy.** | Wykonawca w okresie wdrożenia przeprowadzi w siedzibie Zamawiającego szkolenia dla Administratora systemu. Szkoleniem zostaną objęte osoby wskazane przez Zmawiającego z zakresie dostarczonego rozwiązania teleinformatycznego, co najmniej w zakresie :   * Systemu wirtualizacji. * Systemu backupu. * Firewall   Celem szkolenia administratora będzie zapoznanie się z systemem informatycznym, poznanie poszczególnych funkcji i modułów oraz nauka jego obsługi w praktyce. Na etapie wdrożenia strony ustalą szczegółowy porządek i podział szkoleń z uwzględnieniem wymagań zawartych w niniejszym rozdziale, które przyjęte zostaną w Planie szkoleń.  Wykonawca zobowiązany jest do przeprowadzenia szkoleń w formie instruktażu stanowiskowego dla personelu w podziale na role w Systemie. Taki sposób przeprowadzenia szkoleń jest najbardziej efektywny i umożliwi personelowi rozpoczęcie pracy zaraz po zakończeniu szkolenia. |
|  | **Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.** | Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą.  **Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.**  W tym czasie przedstawiciel Wykonawcy:   * zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. * dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności:  1. wirtualizacji 2. systemu backupu   Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania. |
|  | **Opracowanie dokumentacji powykonawczej** | Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.   1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów. 2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację). 3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały. 5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów. |
|  | **Opieka serwisowa** | Zamawiający wymaga świadczenia opieki serwisowej przez okres 12 miesięcy z czasem reakcji na zaistniałe problemy wynoszącym 8 godziny (NBD). Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych. |

## Diagnoza cyberbezpieczeństwa

|  |
| --- |
| Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina", opisanymi na stronie <https://www.gov.pl/web/cppc/cyfrowa-gmina>  Wykonawca musi wykonać usługę zgodnie zakresem oraz z formularzem stanowiącym załącznik do dokumentacji konkursowej. załączniku nr  Załącznik\_nr\_8\_-\_Formularz\_informacji\_związanych\_z\_przeprowadzeniem\_diagnozy\_cyberbezpieczeństwa  Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. |