Załącznik nr 1 do
Zaproszenia do składania ofert

Or.271.13.2017

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

na: „udostępnienie dla Starostwa Powiatowego w Ciechanowie serwera poczty elektronicznej wraz z jego administracją".

Przedmiotem zamówienia jest świadczenie w okresie od 1 lipca 2017 do 31 grudnia 2019 roku usługi hostingowej polegającej na udostępnieniu dla Starostwa Powiatowego w Ciechanowie indywidualnie skonfigurowanego serwera poczty elektronicznej wraz jego administracją.

Świadczenie usługi będzie realizowane etapami, zgodnie z kolejnością określoną przez Zamawiającego ,tj.:

1) ETAP I - okres przeznaczony na przeprowadzenie przez Wykonawcę wszelkich prac przygotowawczych niezbędnych do świadczenia usługi zgodnie z wymaganiami Zamawiającego. W celu oceny gotowości do świadczenia usługi Wykonawca udostępni Zamawiającemu system poczty (lub jego testową wersję), przy pomocy którego będzie realizowana usługa. Warunkiem zakończenia ETAPU I jest osiągnięcie przez system poczty funkcjonalności wymaganej przez Zamawiającego. Za prace realizowane w ramach ETAPU I Wykonawcy nie przysługuje wynagrodzenie. ETAP I trwa od daty zawarcia umowy na realizację zamówienia do 30 czerwca 2017 roku a w przypadku, gdy Wykonawca nie zrealizuje prac w tym terminie – do zakończenia tych czynności;
2) ETAP II - okres od 1 lipca 2017 roku, jednak nie wcześniej niż od zakończenia ETAPU I do 31 grudnia 2019 roku. W tym okresie Wykonawca będzie świadczył usługę będącą przedmiotem zamówienia, wg „specyfikacji usługi" określonej w dalszej części SOPZ.

„Specyfikacja usługi"

Podstawowym zadaniem Wykonawcy jest doprowadzenie do osiągnięcia celów zamówienia określonych w dalszej części SOPZ. Cele zostały sformułowane, mając na uwadze, że Zamawiający jest organem administracji publicznej, w związku z czym główny nacisk nałożono na:

- zapewnienie monitorowania korzystania z poczty elektronicznej (co i kiedy do urzędu wpłynęło oraz co i kiedy zostało z urzędu wysłane),
- zwiększanie bezpieczeństwa stosując wielopoziomową separację potencjalnie niebezpiecznej poczty oraz zasadę ograniczonego zaufania do użytkowników poczty,
- zapewnienie integralności, dostępności i poufności danych zgromadzonych w poczcie elektronicznej.

Niniejszy SOPZ określa cele, które należy osiągnąć. Zamawiający w żaden sposób nie narzuca sposobu realizacji zamówienia, w tym technologii oprogramowania i sprzętu ani ich ilości i jakości. Określonych celów nie należy traktować jako wymaganego funkcjonalnego podziału oprogramowania a jedynie jako zestaw cech użytkowych, które należy zapewnić. Wykonawca może osiągnąć cele w wybrany przez siebie sposób, bazując na swojej wiedzy i doświadczeniu.

W ramach realizacji zamówienia:

- Wykonawca: odpowiada za dostępność usługi; konfigurację, administrację, zabezpieczanie przed nieautoryzowanym dostępem, atakami intruzów, złośliwym oprogramowaniem, aktualizację oraz monitorowanie poprawności działania, zarówno w zakresie oprogramowania, sprzętu, łączy internetowych i innych niezbędnych do prawidłowego działania usługi. Wykonawca odpowiada także za przechowywanie

zgromadzonych zasobów (np. poczty, logów, konfiguracji), oraz sporządzanie i przechowywanie ich kopi bezpieczeństwa, przeszkolenie administratorów zamawiającego oraz świadczenie im wsparcia technicznego; dokonywanie zmian w konfiguracji usługi w razie wystąpienia potrzeby zgłoszonej przez Zamawiającego. Wykonawca będzie również udzielał Zamawiającemu informacji o stosowanych zabezpieczeniach oraz udostępni dokumentację niezbędną do uzupełniania dokumentacji bezpieczeństwa Zamawiającego,

- Zamawiający: będzie realizował podstawowe czynności administracyjne, które zdaniem Zamawiającego nie powinny angażować Wykonawcy, takie jak: zakładanie kont pocztowych i ich parametryzacja; ustalanie i resetowanie haseł użytkowników; pomoc użytkownikom w pracy z systemem poczty; konfiguracja niektórych ustawień filtracji, o których mowa w dalszej części dokumentu; przeglądanie raportów i statystyk zdarzeń bezpieczeństwa; zasilenie systemu poczty danymi, tj. dotychczas zgromadzoną pocztą elektroniczną oraz książkami adresowymi – czynności te będą przeprowadzać administratorzy zamawiającego (zwani dalej również AZ).

Celami zamówienia są:

1) **zapewnienie dostępu do poczty za pomocą różnych protokołów**: POP3, SMTP, IMAP w tym szyfrowane wersje tych protokołów oraz HTTPS, przy czym podstawowy dostęp do poczty oraz narzędzi administracyjnych będzie przez system typu webmail, osiągany poprzez protokół HTTPS, weryfikowany powszechnie zaufanym certyfikatem. W zabezpieczaniu ruchu HTTPS należy wziąć pod uwagę, że po stronie Zamawiającego urządzenia i systemy antywirusowe skanują ruch SSL podmieniając certyfikaty na własne;

2) **zapewnienie możliwości ograniczenia dostępu do poszczególnych skrzynek pocztowych**: z jakich adresów IP (więcej niż jednego) oraz przy użyciu jakich protokołów (więcej niż jednego) można z danej skrzynki korzystać;

3) **wymuszanie właściwego zachowania użytkowników umożliwiając prowadzenie polityki haseł, zarządzania kontami i sesjami**, poprzez:
   a) automatyczne wylogowanie po zadanym czasie bezczynności,
   b) automatyczną blokadę dostępu do poczty po zadanej ilości nieudanych prób logowania,
   c) wymaganie określonej złożoność haseł (długość / ilość małych liter / wielkich liter / cyfr / znaków specjalnych),
   d) pilnowanie historii użycia haseł – brak możliwość użycia tego samego hasła przez zadany okres czasu,
   e) wygasanie haseł po zadanym okresie ich użycia,
   f) brak możliwości zapamiętania hasła w przeglądarce internetowej;

4) **zapewnienie dedykowanej przestrzeni (folderu lub folderów) dla przykładu zwanej dalej KWARANTANNA,** jednej dla całego serwera poczty, przeznaczonej do przechowywania poczty odrzuconej przez wszystkie mechanizmy filtracji jakie tylko będą zastosowane, do której dostęp będą mieli wyłącznie AZ, którzy będą mogli przenosić wybraną pocztę do skrzynek użytkowników. Poczta z KWARANNTANNY może być automatycznie usuwana po zadanym czasie, jednak musi być przechowywana przez co najmniej 30 dni od jej odebrania. KWARANTANNA musi być tak zbudowana, aby Administratorzy mogli ją przeglądać stosując również sortowanie i filtrowanie widoku jej zawartości, co najmniej po: dacie odebrania (w tym przedział dat), adresie nadawcy (w tym wyrażenia regularne lub kryteria zawiera/nie zawiera), adresie odbiorcy (w tym wyrażenia regularne lub kryteria zawiera/nie zawiera) oraz po przyczynie odfiltrowania poczty – przykładowe oznaczenia poczty są zawarte w dalszej części SOPZ. AZ muszą mieć również możliwość pobierania z KWARANTANNY poczty i załączników, w tym jednym z protokołów POP3 lub IMAP;

5) **ograniczanie użytkownikom dostępu do spamu**, przenosząc takie wiadomości do wcześniej opisanej KWARANTANNY, jednocześnie dodając stosowne oznaczenie, np.

„SPAM". Obecnie sytuacja jest następująca: dotychczasowy dostawca korzysta jednocześnie z RBL, szarych list oraz SPF – i filtry te działając łącznie przepuszczają kilkanaście – kilkadziesiąt szt. spamu dziennie. Wykonawca użyje wybranych przez siebie sposobów rozpoznawania spamu i będzie je modyfikował, gdy okażą się niewystarczające;

6) **ograniczanie użytkownikom dostępu do zainfekowanych wiadomości i załączników,** stosując system antywirusowy (inny niż ESET, Sophos i Cyberoam). Każda poczta rozpoznana jako zagrożenie będzie przenoszona do wcześniej opisanej KWARANTANNY, jednocześnie dodając stosowne oznaczenie, np. „WIRUS";

7) **ograniczanie użytkownikom dostępu do załączników zawierających potencjalnie niebezpieczne elementy** (takie jak makra stosowane w MS Office, skrypty PowerShell i inne), przenosząc takie wiadomości do wcześniej opisanej KWARANTANNY, jednocześnie dodając stosowne oznaczenie, np. „NIEBEZPIECZNY KOD";

8) **ograniczenie użytkownikom dostępu do poczty, do której załączono pliki zabezpieczone hasłem lub zaszyfrowane,** których inspekcji nie można przeprowadzić, przenosząc takie wiadomości do wcześniej opisanej KWARANTANNY, jednocześnie dodając stosowne oznaczenie, np. „ZASZYFROWANY";

9) **umożliwienie administratorom zamawiającego filtracji poczty przychodzącej po dopuszczalnych i niedopuszczalnych rozszerzeniach lub typach załączonych plików** (z obsługą wyrażeń regularnych lub kryteriów zawiera / nie zawiera) oraz przenoszenie takich wiadomości do wcześniej opisanej KWARANTANNY, jednocześnie dodając stosowne oznaczenie, np. „NIEBEZPIECZNY ZAŁĄCZNIK".

   Przykłady:
   - każda wiadomość zawierająca co najmniej jeden plik znajdujący się na liście niepożądanych rozszerzeń zostanie przeniesiona do KWARANTANNY;
   - każda wiadomość zawierająca co najmniej jeden plik nieznajdujący się na liście pożądanych rozszerzeń zostanie przeniesiona do KWARANTANNY;

10) **ograniczenie użytkownikom dostępu do poczty, do której załączono pliki skompresowane do formatu ZIP** (inne formaty plików skompresowanych zostaną umieszczone na liście niedopuszczalnych rozszerzeń), spełniających co najmniej jedno z kryteriów:
    a) bezpośrednio wewnątrz pliku znajdują się pliki, które powinny powodować przeniesienie takiego maila do KWARANTANNY na podstawie warunków filtracji określonych w pkt 6), 7), 8) lub 9),
    b) bezpośrednio wewnątrz którego znajdują się kolejne dowolne pliki skompresowane.

    Przenosząc takie wiadomości do wcześniej opisanej KWARANTANNY należy dodać do nich stosowne oznaczenie, właściwe dla zastosowanego mechanizmu filtracji – 6), 7), 8) lub w nadać oznaczenie „SKOMRESOWANY".

11) **umożliwianie administratorom utworzenie czarnej listy nadawców poczty przychodzącej** określonych przy użyciu wyrażeń regularnych lub kryteriów zawierania określonego ciągu znaków. Poczta pasująca do czarnej listy powinna być przenoszona do wcześniej opisanej KWARANTANNY, jednocześnie dodając stosowne oznaczenie, np. „NIEPOŻĄDANY NADAWCA",

12) **umożliwianie administratorom utworzenie czarnej listy wyrażeń** (ciągów znaków mogących również zawierać polskie litery, znaki specjalne i spacje), których obecność w temacie lub treści wiadomości przychodzącej będzie skutkowało przeniesieniem takiej wiadomości do wcześniej opisanej KWARANTANNY, jednocześnie dodając stosowne oznaczenie, np. „NIEPOŻĄDANE WYRAŻENIE";

13) **umożliwienie administratorom utworzenie białej listy nadawców**, od których poczta nie będzie podlegała żadnym mechanizmom filtracji i będzie doręczana wprost do skrzynek użytkowników. Biała lista nadawców musi mieć najwyższy priorytet przetwarzania. Musi być tworzona przy użyciu wyrażeń regularnych;

14) **ochrona użytkownika przed linkami zawartymi w treści maili przy dostępie do poczty przez system typu webmail.** W ramach tego mechanizmu, należy rozwiązać następującą sytuację: do użytkowników docierają fałszywe maile z DHL, T-Mobile, PocztaPolska itp. Zdarza się, że nie mają załączników a niebezpieczeństwo kryje się jakimś elemencie treści maila, który trzeba kliknąć. Ten mechanizm ochrony ma to uniemożliwić. Problem jest na tyle istotny, że właściwym jest stosowanie tego mechanizmu do wszystkich wiadomości bez badania czy link jest złośliwy czy nie, zakładając zagrożenie w każdym mailu, który trafił do skrzynek użytkowników. Mechanizm może być nakierowany na działanie w folderach użytkowników – przestrzeń KWARANTANNY może, ale nie musi mieć takiego zabezpieczenia. Ten mechanizm:
- nie może zmieniać i usuwać oryginalnego maila, ale jedynie sterować sposobem jego prezentacji,
- musi zapewniać możliwość dostępu do maila, jednak taką, aby dostęp nie był możliwy do uzyskania przypadkowo;

Przykład:
Treść wszystkich wiadomości przychodzących może być wyświetlana jako czysty tekst (konwertowana z oryginału), a oryginalna treść maila może być dostępna pod jakąś opcją w systemie. Być może możliwym jest wyświetlenie treści wiadomości z jednoczesnym usunięciem z niej odnośników i innych aktywnych elementów, które mogą być niebezpieczne. Nie można jednak modyfikować oryginalnego maila, ponieważ może być on potrzebny, np. dla celów dowodowych przy postępowaniach sądowych;

15) **zapewnienie aby administratorzy zamawiającego mogli konfigurować stosowanie poszczególnych mechanizmów filtracji** o których mowa w pkt. od 5) do 12), włączając lub wyłączając ich stosowanie do każdego konta pocztowego

Przykład:
konto abc@ciechanow.powiat.pl – filtracje nr 5-9 i 12 są włączone, nr 10-11 – nie;

16) **zapewnienie funkcjonalności, która pozwoli na odbieranie przez udostępniony przez Wykonawcę system, poczty elektronicznej odbieranej przez zamawiającego na innych serwerach poczty**

Przykład: po podaniu adresu serwera źródłowego, nr portu, protokołu, loginu i hasła poczta jest pobierana, np. do wskazanego konta pocztowego

17) **zapewnienie użytkownikom poczty w systemie webmail, wiedzy o poczcie, która do nich nie dotarła, ponieważ z określonych przyczyn została przeniesiona do KWARANTANNY.** Użytkownik powinien wiedzieć o każdej poczcie do niego adresowanej, która znajduje się w KWARANTANNIE. Sposób prezentowania użytkownikowi informacji o niedoręczonej do niego poczcie nie może dopuszczać do jej otwarcia (dostęp do KWARANTANNY mają wyłącznie AZ), a jedynie wyświetlać takie informacje o tych wiadomościach, które umożliwią ocenę, czy wiadomość jest jednak ważna i trzeba ją odzyskać (np.: data, nadawca, temat, nazwy i rozmiar załączników, podgląd treści), Należy umożliwić użytkownikowi filtrowanie tego widoku co najmniej: po przedziale dat i adresie nadawcy (w tym wyrażenie regularne lub kryteria zawiera / nie zawiera);

Przykład: każdy użytkownik może mieć własny wykaz-widok (np. NIEODEBRANE), który może być wynikiem wyszukiwania (zapytania) w folderze KWARANTANNA

poczty adresowanej do danego użytkownika, przy czym wiadomości znajdujących się na tym wykazie nie można otworzyć,

18) **zapewnienie możliwości monitorowania korzystania z poczty,** w ramach której należy doprowadzić do tego, aby Zamawiający miał wiedzę o każdej poczcie wysłanej z każdego konta: kiedy, który użytkownik, na jakie adresy wysłał maila, jaki był jego temat, jakie pliki były do niego załączone (wraz z ich rozszerzeniami i rozmiarami), kiedy usunięto wiadomość ze skrzynki użytkownika jeśli do tego doszło; oraz o każdej poczcie odebranej: kiedy mail został odebrany, do którego użytkownika był adresowany, jaki był jego temat, jakie pliki były do niego załączone (wraz z ich rozszerzeniami i rozmiarami), jeśli został przeniesiony do KWARANTANNY, dlaczego tak się stało, kiedy został odczytany przez użytkownika, kiedy został usunięty ze skrzynki użytkownika. Projektując ten mechanizm należy wziąć pod uwagę konieczność spełniania również wymagań, że informacje te:
    a) powinny być tak skonstruowane, aby automatycznie wysyłane / odbieranie maile dotyczące informowania o statusie doręczenia były odnotowane, jednak nie stanowiły odrębnych pozycji,
    b) muszą uwzględniać, że poczta może być adresowana do wielu odbiorców,
    c) musi ujawniać ukrytych adresatów, do których wiadomości wysyłają użytkownicy serwera,
    d) muszą być w dostępne w formie tabeli - zestawienia konkretnych informacji a nie bezpośrednio jako logi serwera poczty,
    e) będą obejmowały również pocztę przesyłaną pomiędzy użytkownikami tego serwera,
    f) będą dostępne wyłącznie dla administratorów Zamawiającego,
    g) powinny być dostępne nawet w stosunku do już skasowanych maili, oraz po nadpisaniu / skasowaniu logów serwera,
    h) żadna z informacji nie może zostać usunięta,
    i) powinny umożliwiać wyszukiwanie oraz filtrowanie i sortowanie z uwzględnieniem przedziałów danych (data od - do) i wyrażeń regularnych lub kryteriów zawiera / nie zawiera, a wyniki tych czynności powinny dać się wydrukować i wyeksportować do plików w formacie xls lub xlsx;

19) **dostarczanie Zamawiającemu ilościowo-jakościowej wiedzy o użyciu serwera poczty i wynikach działania każdego mechanizmu filtracji.** Należy doprowadzić do tego, aby Zamawiający, bez codziennego angażowania Wykonawcy, miał:

    a) ilościową wiedzę o dotychczasowym użyciu serwera – stałe zliczanie:
        - ile maili łącznie odebrano (w GB oraz w sztukach),
        - ile maili łącznie wysłano (w GB oraz w sztukach),
        - ile maili wysłały poszczególne konta pocztowe (w GB oraz w sztukach),
        - ile maili odebrały poszczególne konta pocztowe (w GB oraz w sztukach),
        - ile maili łącznie zostało przeniesionych do KWARANTANNY (w GB oraz w sztukach),
        - ile maili zostało przeniesionych do KWARANTANNY z powodu działania poszczególnych mechanizmów filtracji (w GB oraz w sztukach),

    b) ilościową wiedzę o aktualnym użyciu serwera:
        - ile aktualnie poczty znajduje się na serwerze (w GB oraz z sztukach) oraz w rozbiciu na odebrane i wysłane,
        - ile aktualnie poczty znajduje się w KWARANTANNIE (w GB oraz w sztukach),
        - ile aktualnie poczty znajduje się w KWARANTANNIE w rozbiciu na poszczególne mechanizmy filtracji (w GB oraz w sztukach),
        - ile aktualnie poczty znajduje się w folderach poszczególnych użytkowników (w GB oraz w sztukach) oraz w rozbiciu na odebrane i wysłane,

    c) jakościową wiedzę o zdarzeniach w okresie ostatnich 7 i 30 dni:
        - na każdy zastosowany mechanizm filtracji:

-- lista 10 najczęstszych nadawców,
-- lista 10 najczęstszych adresatów,
-- lista 10 najczęstszych przyczyn, np. jeśli wirus to jaki, jeśli niepożądany typ pliku – to jaki, itd.
- lista 10 użytkowników poczty, którzy wysłali najwięcej poczty (w sztukach),
- lista 10 użytkowników poczty, którzy otrzymali najwięcej poczty (w sztukach),

d) informacje o:
- wszystkich kontach, które są zablokowane przez nieudane próby logowania,
- wszystkich kontach, do których nie logowano się dłużej niż 7 dni.

W/w informacje mogą być przygotowane jako predefiniowane raporty lub w formie dedykowanego narzędzia, przy pomocy którego można je utworzyć, wraz z instrukcją i przykładami jego użycia.

20) zapewnienie aby użytkownik konta pocztowego w systemie webmail:
a) posługiwał się wyłącznie podstawowymi folderami poczty (odebrane/wysłane/robocze/kosz),
b) posiadał dostęp do typowych funkcjonalności poczty, jak: wysyłanie do wielu adresatów, przekierowanie, odpowiedź, wysyłanie do ukrytych adresatów, pobranie maila na dysk, zaznaczenie wielu maili jednocześnie, itp.
c) posiadał własną książkę adresową,
d) mógł skonfigurować automatyczną odpowiedź działającą w zadanym okresie czasu (np. w okresie przebywania na urlopie);
e) mógł skonfigurować wstawianie podpisów pod wysyłanym mailem,
f) dysponował automatycznym zapisywaniem tworzonej wiadomości,
g) mógł włączyć / wyłączyć widok wątków wiadomości,
h) bez instalacji dodatkowego oprogramowania mógł załączać wiele plików jednocześnie,
i) miał możliwość sortowania poczty po wszystkich kolumnach oraz wyszukiwania po nadawcy, adresacie, słowach w temacie i treści, przy czym domyślnym sortowaniem jest po kryterium daty – najnowsze wiadomości na górze,
j) nie miał możliwości samodzielnej konfiguracji żadnych parametrów o cechach administracyjnych lub wymagających wiedzy wykraczającej poza wysyłanie/odbieranie poczty - wszelkie tego rodzaju konfiguracje powinny być ustalane przez administratorów zamawiającego;

21) zapewnienie dostępności usługi tj. takiego stanu wszystkich elementów składających się na usługę, który pozwala na wysyłanie i odbieranie poczty przy spełnianiu wszystkich warunków określonych w SOPZ. W ramach osiągania tego celu Wykonawca będzie usuwał wszelkie awarie w ciągu 2 godzin od ich zgłoszenia. Jeśli w celu utrzymania dostępności usługi Wykonawca będzie samodzielnie przeprowadzał okresowe konserwacje, przeglądy, konfiguracje – musi je wykonywać w sposób zachowujący dostępność usługi lub w godzinach nocnych,

22) zapewnienie dostępności i integralności poczty zgromadzonej w ramach realizacji zamówienia, poprzez stosowanie takiego systemu przechowywania danych, który uniemożliwia utratę zgromadzonej poczty elektronicznej oraz informacji o odebranych i wysłanych wiadomościach;

23) zapewnienie, aby system pocztowy udostępniany w ramach świadczenia usługi:
a) pracował w domenie ciechanow.powiat.pl;
b) stosował ten sam i prawidłowy czas dla wszystkich użytkowników oraz do oznaczania zdarzeń. Wykonawca musi uniemożliwić, aby odebrany mail był oznaczony datą wysłania lub odebrania przesuniętą o kilka dni do przodu. Jeśli nie można (albo nie powinno się) modyfikować tych oznaczeń należy wprowadzić dodatkowe pola informujące o stanie faktycznym,

c) umożliwiał odbieranie i wysyłanie poczty o łącznym rozmiarze załączników co najmniej 25MB,
d) pozwalał administratorom na konfigurowanie aliasów kont pocztowych i automatycznego przekierowania poczty na inny adres,
e) zapewniał Zamawiającemu nie współdzielenie reputacji serwera poczty z innymi podmiotami,
f) zapewniał możliwość konfiguracji systemu, aby poczta wysyłana przez wszystkich użytkowników była tworzona w formacie tekstowym,
g) poprawnie działał w najnowszej wersji przeglądarek internetowych Microsoft Edge, Mozilla Firefox i Google Chrome,
h) umożliwiał import dotychczasowych maili (odebranych/wysłanych) wprost z plików programu Mozilla Thunderbird do skrzynek użytkowników, albo np. protokołem IMAP,
i) umożliwiał import książek adresowych poszczególnych użytkowników wprost z programu Mozilla Thunderbird lub innego formatu, do którego eksport obsługuje ten program,
j) zapewniał panel użytkownika poczty, pomoc i wszystkie komunikaty w języku polskim,
k) nie posiadał limitu ilości skrzynek pocztowych,
l) nie posiadał limitu wysłanych i odebranych wiadomości,
m) automatyczne żądał informacji o statusie doręczenia wysyłanej poczty,
n) Wykonawca zapewni taką wydajność i pojemność serwera, która pozwoli na korzystanie świadczenie usługi przez cały okres trwania umowy, w szczególności na przechowywanie całej poczty elektronicznej za wyjątkiem KWARANTANNY, której zawartość może być okresowo usuwana;

W ramach realizacji zamówienia Wykonawca:

1) zapewni również rejestrację domeny ciechanow.powiat.pl, udostępni serwery nazw dla niej oraz zapewni przechowanie jej strefy DNS,
2) udostępni Zamawiającemu przestrzeń nie mniejszą niż 1GB, na serwerze FTP z szyfrowanym połączeniem.

Dodatkowe informacje Zamawiającego o dotychczasowym użyciu poczty:

Zamawiający nie dysponuje szczegółowymi danymi statystycznymi o użyciu dotychczasowego serwera poczty, ale posiada wiedzę, że:

1) w użyciu będzie około 130 skrzynek pocztowych,
2) tylko na ogólny adres poczty Starostwa w okresie od 1 stycznia 2017 do 30 kwietnia 2017 wpłynęło 6085 szt. wiadomości o łącznym rozmiarze 2,5 GB. Wiadomości te zostały odebrane przez klienta poczty po przejściu na serwerze poczty filtrów: RBL, szarych list i SPF. Blisko połowę ilości tej poczty można uznać za bezwartościową. Pozostała poczta jest rozsyłana pomiędzy pracowników Starostwa w ramach domeny, która będzie obsługiwana przez Wykonawcę. Nie posiadamy wiedzy o ilości poczty odrzuconej przez dotychczasowego operatora jako spam lub zawierającej zagrożenia,
3) Starostwo nie prowadzi masowej korespondencji wychodzącej, np. do 200 adresatów,
4) zdarza się, że otrzymujemy pocztę adresowaną również np. do 230 innych jednostek (np. rozsyłaną do określonych jednostek budżetowych w ramach województwa),
5) cała poczta przychodząca i wychodząca, która będzie podlegała migracji do systemu Wykonawcy, zgromadzona dotychczas w klientach poczty ma około 200GB pojemności i obejmuje okres nawet kilku lat. Przed migracją poczta będzie podlegała weryfikacji, w celu usunięcia zbędnych wiadomości.