Umowa nr .....

Zawarta w dniu ................ roku w Nowej Rudzie pomiędzy:

Gminą Nowa Ruda, z siedzibą w Nowej Rudzie ul. Niepodległości 2, 57-400 Nowa Ruda

REGON:890718142, NIP: 885-15-34-651, reprezentowaną przez:

1. ......................................................,

(przy kontrasygnacie Skarbnika Gminy Nowa Ruda),

1. .......................................................,

zwanym dalej „Zamawiającym”

a,

...........................................................

reprezentowanym przez:

1. ......................................................,

zwaną/zwanym dalej „Wykonawcą".

łącznie zwanymi „Stronami”, a odrębnie „Stroną”

w oparciu o przeprowadzone w trybie podstawowym na podstawie art. 275 pkt 2 ustawy z dnia
11 września 2019 r. Prawo zamówień publicznych (Dz. U. 2023 poz. 1605 z późn. zm.) postępowanie o wartości mniejszej niż progi unijne, została zawarta Umowa o następującej treści:

|  |
| --- |
| **§ 1****Przedmiot umowy**1. Przedmiotem umowy jest dostawa systemu ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Zamawiający jest obecnie w posiadaniu systemu ochrony poczty o nr seryjnym FE200E3A17000243.
2. 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.
3. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.
4. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:
5. Tryb Gateway.
6. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
7. System musi być wyposażony w interfejsy: 4 porty Gigabit Ethernet RJ-45.
8. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB .
9. System musi posiadać wbudowany port konsoli szeregowej.
10. Zasilanie z sieci 230V/50Hz.
11. W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.
12. Funkcje serwera poczty. W tym zakresie dostarczony system musi zapewniać:
13. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
14. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2).
15. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
16. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3).
17. Polski interfejs użytkownika przy dostępie przez WebMail.
18. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
19. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.
20. Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:
21. Wsparcie dla co najmniej 20 domen pocztowych.
22. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys wiadomości/godzinę.
23. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
24. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
25. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
26. 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.
27. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
28. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
29. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
30. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
31. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
32. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
33. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
34. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
35. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
36. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
37. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
38. Kontrola antywirusowa i ochrona przed malware. W tym zakresie dostarczony system ochrony poczty musi zapewniać:
39. Skanowanie antywirusowe wiadomości SMTP.
40. Kwarantannę dla zainfekowanych plików.
41. Skanowanie załączników skompresowanych.
42. Definiowanie komunikatów powiadomień w języku polskim.
43. Blokowanie załączników w oparciu o typ pliku.
44. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
45. 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.
46. 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.
47. Ochronę typu wirus outbrake.
48. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.
49. System musi zapewniać poniższe funkcje i metody filtrowania spamu:
50. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
51. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
52. Szczegółowa kontrola nagłówka wiadomości.
53. Analiza Heurystyczna.
54. Współpraca z zewnętrznymi serwerami RBL, SURBL.
55. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
56. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
57. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
58. Kontrola w oparciu o Greylisting oraz SPF.
59. Filtrowanie treści wiadomości i załączników.
60. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
61. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
62. Ochrona typu outbrake.
63. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
64. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
65. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
66. 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.
67. System musi zapewniać poniższe funkcje i metody filtrowania:
68. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
69. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
70. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
71. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
72. Weryfikacja poprawności adresu e-mail nadawcy.
73. Funkcje logowania i raportowania. W tym zakresie dostarczony system ochrony poczty musi zapewniać:
74. Logowanie do zewnętrznego serwera SYSLOG.
75. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
76. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
77. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
78. Możliwość analizy przebiegu sesji SMTP.
79. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
80. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
81. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
82. System ochrony poczty musi zapewniać poniższe funkcje:
83. Konfigurację HA w każdym z trybów: gateway, transparent.
84. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
85. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
86. Monitorowanie stanu pracy klastra.
87. Aktualizacje sygnatur, dostępo do bazy spam. W tym zakresie dostarczony system ochrony poczty musi zapewniać:
88. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
89. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
90. System ochrony poczty musi zapewniać poniższe funkcje:
91. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
92. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
93. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
94. Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:
95. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.
96. Licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 12 miesięcy.
97. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
98. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden inżynier musi posiadać najwyższy stopień certyfikacji dla danego rozwiązania) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty.
99. Wykonawca zapewnia wsparcie techniczne rozwiązania w zakresie:
100. wsparcie techniczne certyfikowanych inżynierów Fortinet
101. system helpdesk z historią ticketu oraz wszystkich zrealizowanych zgłoszeń
102. certyfikacja ISO 9001
103. pomoc przy rejestracji urządzeń
104. zakładanie zgłoszeń serwisowych u producenta
105. pomoc w procesie realizacji naprawy i wymiany urządzeń w ramach gwarancji producenta
106. doradztwo w zakresie konfiguracji
107. podwyższony priorytet obsługi zgłoszeń
108. możliwość zmiany priorytetu zgłoszenia w systemie producenta
109. zdalna rekonfiguracja urządzenia (połączenie szyfrowane, do 10 zgłoszeń)
110. szkolenie zdalne z konfiguracji urządzenia dla jednej osoby
 |
| **§2****Warunki dostawy**1. Urządzenie będące przedmiotem umowy wraz licencjami zostanie dostarczone na adres Zamawiającego w terminie **do … dni od daty podpisania umowy.**
2. Za datę wykonania umowy uważa się datę podpisania protokołu odbioru dostawy wraz z protokołem odbioru instalacji oprogramowania i przeszkolenia pracownika Zamawiającego w zakresie jego obsługi - z uwzględnieniem terminu określonego w §2 pkt. 1 umowy.
 |
| **§ 3****Cena i warunki płatności**1. Zamawiający zobowiązuje się zapłacić jednorazowo za realizację przedmiotu umowy, o którym mowa w § 1, cenę **……………… zł** **netto** + VAT 23% – łącznie **……………zł brutto** (słownie: ……………………………….. złotych i …./100).
2. Niedoszacowanie, pominięcie oraz brak rozpoznania zakresu przedmiotu umowy nie może być podstawą do żądania zmiany wynagrodzenia ryczałtowego określonego w ust. 1 niniejszego paragrafu.
3. Płatność będzie dokonywana przelewem na wskazany przez Wykonawcę rachunek bankowy, w terminie **[…]** dni od daty otrzymania prawidłowo wystawionej faktury wraz z zatwierdzonym protokołem odbioru.
4. Wykonawca oświadcza, że numer rachunku rozliczeniowego wskazany we wszystkich fakturach, które będą wystawione w jego imieniu, jest rachunkiem/nie jest rachunkiem\* dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - Prawo Bankowe prowadzony jest rachunek VAT.
5. Jeśli numer rachunku rozliczeniowego wskazany przez Wykonawcę jest rachunkiem, dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - Prawo Bankowe prowadzony jest rachunek VAT to:
6. Zamawiający oświadcza, że będzie realizować płatności za faktury z zastosowaniem mechanizmu podzielonej płatności tzw. split payment.
7. Podzieloną płatność tzw. split payment stosuje się wyłącznie przy płatnościach bezgotówkowych, realizowanych za pośrednictwem polecenia przelewu lub polecenia zapłaty dla czynnych podatników VAT. Mechanizm podzielonej płatności nie będzie wykorzystywany do zapłaty za czynności lub zdarzenia pozostające poza zakresem VAT (np. zapłata odszkodowania), a także za świadczenia zwolnione z VAT, opodatkowane stawką 0%.
8. Za nieterminowe płatności faktur, Wykonawca ma prawo naliczyć odsetki ustawowe za opóźnienie.
9. Cesja wierzytelności wynikająca z niniejszej umowy może nastąpić jedynie za zgodą Zamawiającego za pisemną zgodą Zamawiającego.
10. Za dzień zapłaty uznany będzie dzień dokonania obciążenia rachunku bankowego Zamawiającego.
 |
| **§ 4**GWARANCJA I RĘKOJMIA1. Niezależnie od usługi wsparcia oraz usługi wdrożeniowej - Wykonawca udziela Zamawiającemu gwarancji jakości producenta na dostarczone urządzenia wskazane w par. 1 ust. 1 umowy - zwanej dalej „Gwarancją” na okres 3 lat od dnia podpisania bez uwag protokołu odbioru.
2. Wady w Przedmiocie Umowy ujawnione w okresie gwarancji i rękojmi Wykonawca jest zobowiązany usunąć w terminie wskazanym przez Zamawiającego, nie krótszym niż 3 dni kalendarzowe i nie dłuższym niż 21 dni kalendarzowych - chyba,że zpowodów technologicznych wymagany będzie okres dłuższy, który zostanie uprzednio ustalony z Zamawiającym. Usunięcie wad Wykonawca zgłasza do odbioru Zamawiającemu pisemnie.
3. W razie nieusunięcia we wskazanym terminie przez Wykonawcę wad i usterek stwierdzonych przy odbiorze końcowym, w okresie gwarancji oraz przy przeglądzie gwarancyjnym, Zamawiający jest upoważniony do ich usunięcia na koszt i ryzyko Wykonawcy.
4. Zamawiający będzie korzystał z adresu e-mail Wykonawcy: […], służącego do zgłaszania awarii lub usterek.

**§ 5****Kary umowne**1. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wartości netto umowy, w przypadku odstąpienia od niniejszej umowy przez Wykonawcę oraz w sytuacji odstąpienia od niniejszej umowy przez Zamawiającego z winy Wykonawcy, z przyczyn leżących po stronie Wykonawcy.

Wykonawca zapłaci karę umowną na podstawie wystawionej przez Zamawiającego noty księgowej, w terminie 14 dni od daty jej doręczenia.1. W razie zwłoki w -realizacji Przedmiotu Umowy Wykonawca zobowiązany jest do zapłacenia kary umownej w wysokości 0,5% wartości netto umowy za każdy rozpoczęty dzień zwłoki, liczony od następnego dnia od upływu terminu określonego w § 2 ust. 1 niniejszej umowy.
2. Zamawiający jest zobowiązany zapłacić Wykonawcy odsetki ustawowe za zwłokę w zapłacie ustalonej ceny liczonej od dnia następnego po dniu, w którym zapłata miała być dokonana.
 |
| **§6****Postanowienia końcowe** |
| 1. Zamawiający oświadcza, że wyraża zgodę na przetwarzanie danych osobowych, udostępnionych w złożonych dokumentach w celu realizacji umowy, zgodnie z art. 5, 6, 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. (RODO).
2. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy kodeksu cywilnego.
3. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej w postaci aneksu pod rygorem nieważności.
4. Spory wynikłe na tle realizacji umowy będą rozstrzygane przez Sąd właściwy dla siedziby Zamawiającego.
5. Umowa została sporządzona w 2 jednobrzmiących egzemplarzach, w tym 1 egzemplarz dla każdej strony.
 |
|  **WYKONAWCA ZAMAWIAJĄCY** |