**Załącznik 20 Wymagania na dostawę i instalację Systemu antywirusowego**

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa do siedziby Zamawiającego **40** sztuk licencji Systemu antywirusowego przeznaczonego dla Komputerów PC opisanych w Załączniku 12, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz ich instalacja i konfiguracja.

**System antywirusowy musi spełniać następujące wymagania funkcjonalne:**

1. Skanowanie antywirusowe plików i wiadomości SMTP.
2. Kwarantanna 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 15 polityk kontroli antywirusowej per system.
7. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u.
8. 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. System musi zapewniać poniższe funkcje i metody filtrowania spamu:
10. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
11. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
12. Szczegółowa kontrola nagłówka wiadomości.
13. Analiza Heurystyczna.
14. Współpraca z zewnętrznymi serwerami RBL, SURBL.
15. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
16. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
17. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
18. Kontrola w oparciu o Greylisting oraz SPF.
19. Filtrowanie treści wiadomości i załączników.
20. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
21. Możliwość zdefiniowania nie mniej niż 15 polityk kontroli antyspamowej per system.
22. Ochrona typu outbrake.
23. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
24. 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.
25. Wymagana wykupiona opieka aktualizacyjna dostarczonego oprogramowania na okres 36 miesięcy od daty Protokołu Odbioru Końcowego.