CENTRALNY OŚRODEK BADANIA ODMIAN ROŚLIN UPRAWNYCH
RESEARCH CENTRE FOR CULTIVAR TESTING
Słupia Wielka 34, PL 63-022 SŁUPIA WIELKA, tel.: (+48) 61 285 23 41, faks: (+48) 61 285 35 58, e-mail: sekretariat@coboru.gov.pl
www.coboru.gov.pl

Słupia Wielka, dnia 27.10.2020 r.

Nr sprawy: ZP/TCZ/14/2020

OGŁOSZENIE

ZAPYTANIE OFERTOWE

Centralny Ośrodek Badania Odmian Roślin Uprawnych z siedzibą w Słupi Wielkiej, zaprasza do złożenia oferty w postępowaniu na **„Dostawę (zakup) systemu zabezpieczenia poczty"** prowadzonym zgodnie z warunkami określonymi w załączonym zapytaniu ofertowym.

Informujemy, że niniejsze zapytanie ofertowe nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, ani zapytanie ofertowe w rozumieniu ustawy Prawo Zamówień Publicznych.

Z-ca DYREKTORA
ds. administracyjno-ekonomicznych
mgr Arkadiusz Sokołowski

.....
(podpis osoby upoważnionej)

Załącznik nr 2

do Zarządzenia 10/2016

CENTRALNY OŚRODEK (09)
BADANIA ODMIAN ROŚLIN UPRAWNYCH
Słupia Wielka 34
63-022 Słupia Wielka
tel. 61 285 23 41 fax 61 285 35 58
NIP: PL7861697911 REGON: 301631408

Słupia Wielka, dnia 27.10.2020r.

.....

(pieczęć zamawiającego)

ZAPYTANIE OFERTOWE

(niniejsze zapytanie nie stanowi zapytania ofertowego

w rozumieniu przepisów PZP)

Zakup i dostawa systemu zabezpieczenia poczty

Zwracam się z prośbą o przedstawienie swojej oferty na poniżej opisany przedmiot zamówienia:

1. Przedmiot zapytania ofertowego obejmuje:
    a. Dostawę systemu zabezpieczenia poczty
    b. Świadczenie usług gwarancyjnych i wsparcia technicznego 24/7 oraz aktualizacji baz zagrożeń bezpieczeństwa producenta dla dostarczonego Sprzętu oraz Oprogramowania przez okres co najmniej 24 miesięcy
2. Wymagania dotyczące systemu

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników systemu poczty elektronicznej Microsoft Exchange Server 2016 .

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych. Zamawiający nie dopuszcza systemu w postaci maszyny wirtualnej.

Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń.

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o

obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym z trybów:

1. Tryb gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi być wyposażony w 4 porty Gigabit Ethernet RJ-45.
2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB.
3. System musi posiadać wbudowany port konsoli szeregowej.
4. 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. 30 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 oraz POP3.
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. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Prevention).
18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
19. Możliwość integracji z Office 365 oraz oprogramowaniem Microsoft Exchange Server 2016 z wykorzystaniem API.

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 virusoutbreak.
10. 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.

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 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 outbreak.

14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level).
17. 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.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona 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.
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 mieć możliwość konfiguracji poniższych funkcji:

1. Konfiguracji HA w każdym z trybów: gateway, transparent.
2. Trybu synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywania awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowania 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. 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

1. VBSpam and VB100 rated lub Common Criteria NDPP,
2. 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: 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 minimum 24 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji baz zagrożeń bezpieczeństwa producenta, aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Termin realizacji zamówienia: Zamawiający wymaga aby dostawa wraz z **maksymalnie do 15 grudnia 2020 roku od dnia podpisania umowy (złożenia zamówienia)**

Ofertę (zgodną z załącznikiem) prosimy:

- złożyć osobiście lub przesłać pocztą na adres:

  Centralny Ośrodek Badań Odmian Roślin Uprawnych w Słupi Wielkiej,

  Słupia Wielka 34,

  63-022 Słupia Wielka , lub
- drogą elektroniczną na adres e-mail: a.nowicka@coboru.gov.pl,
- osoba do kontaktu mgr Arkadiusz Sokołowski, tel. 61 285 23 41 w. 210

w terminie do 05 listopada 2020 roku do godziny 10.00

Kryteria

Zamawiający wybierze do realizacji ofertę przedstawiającą najkorzystniejszy bilans ceny, parametrów technicznych oraz zadeklarowanego okresu trwania gwarancji, wsparcia technicznego i aktualizacji baz zagrożeń bezpieczeństwa producenta

Zamawiający zastrzega sobie prawo unieważnienia prowadzonego postępowania obejmującego niniejsze zapytanie – bez podawania przyczyny. Wykonawcy nie przysługuje prawo dochodzenia roszczeń w związku z unieważnieniem postępowania, w tym także kosztów poniesionych przez wykonawcę w związku z przygotowaniem i dostarczeniem oferty.

Z-ca DYREKTORA
ds. administracyjno-ekonomicznych

mgr Arkadiusz Sokołowski

.....

(podpis Kierownika Zamawiającego)

Załącznik do zapytania ofertowego

FORMULARZ OFERTOWY WYKONAWCY

Dane dotyczące wykonawcy
Nazwa: .....
Siedziba: .....
Adres poczty elektronicznej: .....
Strona internetowa: .....
Numer telefonu: .....
Numer faksu: ....
Numer REGON: .....
Numer NIP: .....

Dane dotyczące Zamawiającego
Centralny Ośrodek Badania Odmian Roślin Uprawnych
Słupia Wielka 34
63-022 Słupia Wielka
Woj. Wielkopolskie

Zobowiązania wykonawcy
Nawiązując do zapytania ofertowego, którego przedmiotem jest **dostawa systemu zabezpieczenia poczty** oferujemy wykonanie zamówienia za cenę:

Całkowita cena oferty

cena netto.....zł

(słownie: .....)

podatek Vat (23 %) ..... zł

cena brutto .....zł

(słownie: .....)

Oświadczam, że:

- Przedmiot zamówienia zrealizuję w terminie przewidzianym na dzień ..... ***(maksymalnie do 15 grudnia 2020 r.)***

Marka			
	proszę podać nazwę marki		
Nazwa modelu			
	proszę podać nazwę modelu		
Cena (całkowita)	***Cena netto***	***Podatek VAT***	***Cena brutto***

Oświadczam, że oferowany system zabezpieczenia poczty spełnia poniższe wymagania

l.p.	Wymagania minimalne	Oferowany parametr
1.	Dostarczone rozwiązanie musi mieć możliwość pracy w każdym z trybów: 1. Tryb gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).	Spełnia/nie spełnia
2.	**Parametry fizyczne systemu antyspamowego** 1. System musi być wyposażony w 4 porty Gigabit Ethernet RJ-45. 2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB. 3. System musi posiadać wbudowany port konsoli szeregowej. 4. Zasilanie z sieci 230V/50Hz.	Spełnia/nie spełnia
3.	**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. 30 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.	Spełnia/nie spełnia

	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 oraz POP3. 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. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Prevention). 18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. 19. Możliwość integracji z Office 365 oraz oprogramowaniem Microsoft Exchange Server 2016 z wykorzystaniem API.	
4.	**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	Spełnia/nie spełnia

	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 virusoutbreak. 10. 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.	
5.	**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 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 outbreak.	Spełnia/nie spełnia

	14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata. 16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level). 17. 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.	
6.	**Ochrona przed atakami na usługę poczty** System musi zapewniać poniższe funkcje i metody filtrowania: 1. Ochrona przed atakami na adres odbiorcy. 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona anty-spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy.	Spełnia/nie spełnia
7.	**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. 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.	Spełnia/nie spełnia

	8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.	
8.	**Funkcje pracy w trybie wysokiej dostępności (HA)** System ochrony poczty musi mieć możliwość konfiguracji poniższych funkcji: 1. Konfiguracji HA w każdym z trybów: gateway, transparent. 2. Trybu synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywania awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowania stanu pracy klastra.	Spełnia/nie spełnia
9.	**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.	Spełnia/nie spełnia
10.	**Zarządzanie** System ochrony poczty musi zapewniać poniższe funkcje: 1. 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.	Spełnia/nie spełnia
11.	**Certyfikaty** 1. VBSpam and VB100 rated lub Common Criteria NDPP,	Spełnia/nie spełnia

	FIPS 140-2 Certified.	
12.	**Serwisy i licencje** W ramach postępowania powinny zostać dostarczone 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 minimum 24 miesięcy. -	Spełnia/nie spełnia
13.	**Gwarancja oraz wsparcie** System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji baz zagrożeń bezpieczeństwa producenta, aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	Spełnia/nie spełnia

- **Okres udzielonej gwarancji i wsparcia .....m-cy (min. 24 m-ce)**

- Przedmiot zamówienia zostanie dostarczony do siedziby COBORU, Słupia Wielka 34, 63-022 Słupia Wielka. Dostawa odbędzie się transportem Wykonawcy, od poniedziałku do piątku w godz. 7^{00}-15^{00}. Koszt transportu należy wkalkulować w cenę oferty. Zamawiający nie poniesie z tego tytułu żadnych dodatkowych kosztów. Zamawiający wymaga, aby przy dostawie obecna była osoba od strony Wykonawcy, która będzie upoważniona do podpisania protokołu przekazania-odbioru.

Oświadczenie

1. Oświadczam, że zapoznałem się z opisem przedmiotu zamówienia, nie wnoszę żadnych zastrzeżeń oraz uzyskałem niezbędne informacje do przygotowania oferty.
2. Oświadczam, że załączone postanowienia do zapytania ofertowego umowa/wzór umowy zostały przeze mnie zaakceptowane bez zastrzeżeń i zobowiązuję się w przypadku wyboru mojej oferty do zawarcia umowy w miejscu i terminie wyznaczonym przez zamawiającego.

.....

(data i czytelny podpis Wykonawcy)

UMOWA DOSTAWY- wzór

nr ZP/TCZ//2020

zawarta w Słupi Wielkiej, w dniu .... roku

pomiędzy:

Centralnym Ośrodkiem Badania Odmian Roślin Uprawnych

z siedzibą w

Słupia Wielka 34, 63-022 Słupia Wielka

NIP 786-16-97-911

zwanym dalej „Zamawiającym",

reprezentowanym przez:

Zastępcę Dyrektora ds. Ekonomiczno-Administracyjnych

Arkadiusza Sokołowskiego,

działającego na podstawie pełnomocnictwa 18/P/20 z dnia 23 czerwca 2020 roku, którego kopia stanowi załącznik do niniejszej umowy

a

.....

NIP:..... zwanym w dalszej części umowy „Wykonawcą"

reprezentowaną przez:

.....

§ 1. DEFINICJE

1.1. **Dzień roboczy – oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy na terytorium Rzeczypospolitej Polskiej;**

1.2. **Miejsce dostawy –** oznacza siedzibę Centralnego Ośrodka, w którym zostaną zainstalowane Produkty;

1.3. **Sprzęt – oznacza sprzęt dostarczany przez Wykonawcę Zamawiającemu na podstawie niniejszej Umowy, którego szczegółowy wykaz stanowi Załącznik nr 1 do Umowy;**

1.4. **Oprogramowanie – oznacza oprogramowanie niezbędne do prawidłowego funkcjonowania urządzenia, na którego używanie udzielona zostanie na rzecz Zamawiającego licencja;**

1.5. **Produkty** – oznacza Sprzęt i Oprogramowanie dostarczane lub licencjonowane na podstawie niniejszej Umowy, określone w Załączniku nr 1 do Umowy;

1.6. **Usługi gwarancyjne** - oznacza usługi świadczone w stosunku do Sprzętu zgodnie z poziomem usług określonym w Załączniku 2 do Umowy;

1.7. **Wsparcie techniczne** - oznacza usługi świadczone dla zainstalowanego Sprzętu i Oprogramowania;

1.8. **Załącznik** – oznacza załącznik do niniejszej Umowy.

§ 2. PRZEDMIOT UMOWY

2.1. Przedmiot Umowy stanowi:

- Zakup i dostawa systemu zabezpieczenia poczty– 1 szt.
- świadczenie usług gwarancyjnych i wsparcia technicznego 24/7 oraz aktualizacji baz zagrożeń bezpieczeństwa producenta dla dostarczonego Sprzętu oraz Oprogramowania przez okres co najmniej 24 miesięcy

2.2. Termin wykonania zamówienia ustala się do dnia .....

2.3. Wykonawca z uwagi na kwestie organizacyjne oraz charakter przedmiotu zamówienia poinformuje Zamawiającego o terminie dostawy na co najmniej 3 dni robocze przed planowaną dostawą.

§ 3. ZOBOWIĄZANIA WYKONAWCY

3.1. Wykonawca zobowiązuje się do dostarczenia Produktów, świadczenia Usług gwarancyjnych i wsparcia technicznego.

3.2. Wykonawca wyznaczył przedstawiciela właściwie umocowanego do reprezentowania Wykonawcy w zakresie spraw związanych z niniejszą Umową i odpowiedzialnego za kontakty z Zamawiającym oraz kierowanie wykonaniem przedmiotu Umowy.

3.3. Osobą upoważnioną do kontaktów ze strony Wykonawcy jest :

.....

3.4. Wykonawca jest uprawniony do zmiany w każdym czasie osoby wskazanej na podstawie niniejszego punktu, za pisemnym powiadomieniem Zamawiającego.

§ 4. ZOBOWIĄZANIA ZAMAWIAJĄCEGO

4.1. Zamawiający zobowiązuje się do dokonania odbioru i zapłaty za dostarczone Produkty oraz za świadczone Usługi gwarancyjne i wsparcie techniczne (w cenie Produktów).

4.2. Zamawiający przyznaje, że zdolność Wykonawcy do zrealizowania przedmiotu Umowy zależy od pełnej i terminowej współpracy Zamawiającego z Wykonawcą, a także od dokładności i kompletności wszelkich informacji i danych dostarczonych Wykonawcy przez Zamawiającego. Wobec powyższego Zamawiający w szczególności:

a) zapewni dostęp i możliwość wykorzystania wszelkich informacji określonych przez Wykonawcę, jako potrzebne dla prawidłowej realizacji Umowy;

b) w przypadku świadczenia usług przez Wykonawcę w siedzibie Zamawiającego, zapewni warunki potrzebne dla prawidłowej realizacji usług (zapewnienie miejsca do pracy, dostępu do sprzętu komputerowego i oprogramowania, dostępu do sieci telefonicznej i teleinformatycznej);

c) zapewni Wykonawcy dostęp do osób, które zostały delegowane do realizacji, przedmiotu Umowy, zapewni ich obecność w trakcie prac, dostarczy w odpowiednim terminie informacje niezbędne do prowadzenia prac oraz zapewni pracownikom Wykonawcy i innym osobom oddelegowanym przez Wykonawcę do wykonania prac, środowisko pracy u Zamawiającego potrzebne dla prawidłowej realizacji tych prac;

d) zobowiązuje się udostępnić środowisko określone przez Wykonawcę jako potrzebne do wykonania zobowiązań Wykonawcy wynikających z niniejszej Umowy, w szczególności sprzęt i oprogramowanie potrzebne do prawidłowego wykonania przedmiotu Umowy.

4.3. Zamawiający wyznaczył przedstawiciela właściwie umocowanego do reprezentowania w zakresie spraw związanych z realizacją niniejszej Umowy i odpowiedzialnego za kontakty z Wykonawcą, a w szczególności umocowanego do podpisywania protokołów odbiorów przewidzianych Umową, oraz kierowanie wykonaniem przedmiotu Umowy, w tym również uprawnionego do podpisywania protokołów wynikających z niniejszej Umowy. Osobą upoważnioną do kontaktów ze strony Zamawiającego jest :

.....

4.4. Zamawiający jest uprawniony do zmiany w każdym czasie osoby wskazanej na podstawie niniejszego punktu, za pisemnym powiadomieniem Wykonawcy.

§ 5. CENA I WARUNKI PŁATNOŚCI

5.1. Łączna należność Wykonawcy z tytułu wykonania Umowy wynosi netto ..... Do powyższej kwoty zostanie doliczony podatek od towarów i usług VAT 23% w wysokości ..... Łączna należność Wykonawcy wynosi .....

5.2. Wynagrodzenie za usługi gwarancyjne oraz co najmniej 2-letnie wsparcie systemowe zawarte jest w cenie Produktów.

5.3. Wykonawca wystawi fakturę VAT za przedmiot Umowy w terminie 7 dni od dnia podpisania protokołu odbioru, zgodnie z paragrafem 6 niniejszej Umowy.

5.4. Zamawiający zobowiązany jest dokonać płatności w terminie 21 dni licząc od dnia doręczenia prawidłowo wystawionej faktury VAT.

5.5. Wszystkie należności na rzecz Wykonawcy z tytułu realizacji przedmiotu Umowy płatne będą przelewem na rachunek bankowy Wykonawcy nr ..... metodą podzielonej płatności.

5.6. Za dzień zapłaty wynagrodzenia Strony przyjmują datę złożenia polecenia przelewu w banku Zamawiającego.

5.7. Wykonawca, który jest podatnikiem VAT czynnym, oświadcza, że ww. rachunek będzie zgłoszony w urzędzie skarbowym właściwym dla rozliczeń podatkowych Wykonawcy i będzie figurował na białej liście podatników czynnych VAT, a w przypadku jakichkolwiek zmian zobowiązuje się pisemnie powiadomić o tym Zamawiającego, pod rygorem zapłaty na rzecz Zamawiającego kary umownej odpowiadającej wysokości przelewu dokonanego na podany przez Wykonawcę rachunek bankowy nieuwidoczniony na białej liście, z zastrzeżeniem prawa do dochodzenia odszkodowania w pełnej wysokości. W przypadku gdy Zamawiający dokona weryfikacji rachunku bankowego Wykonawcy i okaże się, że ww. rachunek albo ostatnio podany przez Wykonawcę nie figuruje na białej liście, płatność dokonana na którykolwiek ze zgłoszonych w urzędzie skarbowym rachunek bankowy Wykonawcy, stanowi wykonanie zobowiązania Zamawiającego co do zapłaty wierzytelności Wykonawcy

5.8. Zamawiający oświadcza, że jest uprawniony do otrzymywania faktur VAT, posiada NIP 7861997911 i upoważnia Wykonawcę do wystawiania faktur bez podpisu odbiorcy.

§ 6. DOSTAWA I ODBIÓR

6.1. Produkty zostaną dostarczone do siedziby COBORU w Słupi Wielkiej.

6.2. Produkty, o których mowa w § 2 niniejszej umowy powinny być:

a) kompletne,

b) oznakowane przez Producenta w taki sposób, aby możliwa była identyfikacja produktu, jak i Producenta,

c) dopuszczone do obrotu na terenie Polski oraz posiadać wszelkie wymagane przepisami prawa certyfikaty, świadectwa, atesty, deklaracje zgodności i spełniać wszelkie określone prawem wymogi bezpieczeństwa użytkowania,

d) zaopatrzone w wymaganą przepisami prawa dokumentację w języku polskim (tj. certyfikat jakości, instrukcję obsługi, kartę gwarancyjną zawierającą min. numer seryjny, dokument gwarancyjny, termin i warunki gwarancji),

e) zaopatrzone w dokumenty licencji na Oprogramowanie w języku polskim.

6.3. Po montażu Produktów w szafie montażowej wskazanej przez przedstawiciela zamawiającego i uruchomieniu zostanie obustronnie podpisany Protokół Odbioru Produktów. Ryzyko zniszczenia, uszkodzenia lub utraty danego Produktu przechodzi na Zamawiającego w chwili zainstalowania i uruchomienia Produktu w szafie montażowej wskazanej przez przedstawiciela Zamawiającego.

§ 7. WARUNKI GWARANCJI I WSPARCIA TECHNICZNEGO

7.1 Wykonawca udziela gwarancji na sprzęt i wsparcia technicznego na Oprogramowanie .

7.2 Gwarancja Wykonawcy obejmuje wady projektowe, materiałowe oraz wady w wykonaniu Sprzętu. Jeżeli Wykonawca zostanie powiadomiony o takich wadach w okresie gwarancyjnym, Wykonawca według własnej oceny albo naprawi, albo wymieni wadliwy Sprzęt. Wymienione części stają się własnością Wykonawcy. Wymieniane części będą fabrycznie nowe.

7.3 Wykonawca gwarantuje, że Oprogramowanie nie zawiedzie przy wykonywaniu zaprogramowanych czynności z powodu wad materiałowych nośnika. Jeżeli Wykonawca zostanie powiadomiony o wadach Oprogramowania w okresie świadczenia usług wsparcia technicznego, Wykonawca, zgodnie ze swoją oceną podejmie niezwłocznie kroki zmierzające do usunięcia lub zneutralizowania powyższych wad. Wykonawca nie gwarantuje, że Oprogramowanie będzie działało w powiązaniu z każdą kombinacją sprzętu komputerowego i oprogramowania wybraną przez Zamawiającego. Wykonawca nie gwarantuje też, że działanie oprogramowania będzie niezakłócone i bezbłędne.

7.4 Okres gwarancji na sprzęt i wsparcie techniczne na Oprogramowanie wynosi ..... licząc w każdym wypadku od daty podpisania Protokołu Odbioru Produktów.

7.5 Zamawiający może zgłaszać incydenty dotyczące sprzętu i oprogramowania wbudowanego 24 godziny na dobę, przez 7 dni w tygodniu telefonicznie na nr ..... lub drogą elektroniczną na adres e-mail..... . Wykonawca niezwłocznie potwierdzi drogą elektroniczną otrzymanie zgłoszenia awarii. Jeżeli Wykonawca nie potwierdzi otrzymania takiego zgłoszenia, zamawiający będzie domniemywał, że dotarło ono do Wykonawcy, chyba, że udowodni on, że z przyczyn technicznych było to niemożliwe.

7.6 Czas reakcji na zgłoszenie problemu sprzętowego lub problemu z oprogramowaniem wbudowanym i narzędziowym wynosi 4 godziny.

7.7 Usługi będą świadczone w Miejscu instalacji lub zdalnie, zgodnie z oceną Wykonawcy.

7.8 O sposobie usunięcia wady decyduje Wykonawca. Jeżeli w wykonaniu swoich obowiązków gwarant dostarczył uprawnionemu z gwarancji zamiast rzeczy wadliwej rzecz wolną od wad albo dokonał istotnych napraw rzeczy objętej gwarancją, termin gwarancji biegnie na nowo od chwili dostarczenia rzeczy wolnej od wad lub zwrócenia rzeczy naprawionej. Jeżeli gwarant wymienił część rzeczy, przepis powyższy stosuje się odpowiednio do części wymienionej. W

innych wypadkach termin gwarancji ulega przedłużeniu o czas, w ciągu którego wskutek wady rzeczy objętej gwarancją uprawniony z gwarancji nie mógł z niej korzystać.

7.9 Wykonawca w okresie wsparcia technicznego, udostępni uaktualnione wersje Oprogramowania , na używanie którego Zamawiający uzyskał licencję na podstawie niniejszej Umowy. Licencja na ich używanie jest zawarta w cenie Produktów objętych niniejszą Umową.

7.10 Usługi dla danego Produktu będą świadczone zgodnie z poziomem i na zasadach określonych w Załączniku nr 1 do Umowy.

7.11 W ramach obsługi gwarancyjnej i wsparcia technicznego Wykonawca zapewnia fachową kadrę, wszystkie części zamienne i materiały niezbędne do konserwacji i utrzymania Sprzętu w dobrym stanie.

7.12 Wykonawca nie jest zobowiązany w ramach niniejszej Umowy do świadczenia Usług gwarancyjnych lub wsparcia technicznego w przypadku:

- modyfikacji wprowadzonych przez Zamawiającego lub osobę trzecią bez zgody Wykonawcy;
- jeżeli Zamawiający nie pozwoli Wykonawcy na wprowadzenie uzasadnionych ulepszeń technicznych w Produktach;
- niewłaściwej eksploatacji Produktów;
- zmiany miejsca instalacji bez zgody Wykonawcy;
- nie zapewnienia przez Zamawiającego możliwości świadczenia przez Wykonawcę Usług gwarancyjnych lub wsparcia technicznego zgodnie z zasadami określonymi w niniejszej Umowie;
- okoliczności siły wyższej lub innych okoliczności, za które Wykonawca nie ponosi odpowiedzialności.

7.13 Zamawiający udzieli Wykonawcy dostępu do Produktów objętych niniejszą Umową i umożliwi użycie wyposażenia i środków niezbędnych do ich obsługi niezwłocznie po przybyciu przedstawiciela Wykonawcy.

§ 8. WARUNKI UDZIELANIA LICENCJI NA OPROGRAMOWANIE

8.1 Wszelkie licencje dotyczące Oprogramowania zostają udzielone przez Wykonawcę na poniższych warunkach:

a) po dokonaniu odbioru Oprogramowania , zgodnie z postanowieniami Umowy, Wykonawca przyznaje Zamawiającemu niewyłączną, nieprzenoszalną, rozciągającą się na całe terytorium Rzeczypospolitej Polskiej, licencję, na czas nieoznaczony do używania Oprogramowania i związanej z nim dokumentacji oraz uaktualnień, na sprzęcie komputerowym, dla którego Oprogramowanie jest dostarczone na

następujących polach eksploatacyjnych: przechowanie, ładowanie, instalacja, uruchamianie i wyświetlanie. Zamawiający nie może modyfikować, dezasemblować ani dekompilować oprogramowania w zakresie i na warunkach innych niż określone w art. 75 ust. 2 i 3 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, (Dz.U. z 2000 r. Nr 80, poz. 904). Zamawiający poinformuje Wykonawcę o każdej zamierzonej dezasemblacji lub dekompilacji;

b) jeżeli przepisy prawa nie stanowią inaczej, wszelkie inne prawa majątkowe dotyczące Oprogramowania i dokumentacji przysługują Wykonawcy;

c) Zamawiający może kopiować Oprogramowanie i dokumentację jedynie w celach archiwalnych, w celu wymiany wadliwej kopii lub w celu zweryfikowania błędów w programie;

d) wszystkie kopie Oprogramowania lub ich części oraz dokumentacja zostaną przez Zamawiającego opatrzone znakami zastrzegającymi prawa autorskie, którymi opatrzone są oryginalne wersje Oprogramowania;

e) Zamawiający nie będzie sprzedawał, udzielał podlicencji ani w żaden inny sposób udostępniał osobom trzecim oryginalnej wersji ani kopii Oprogramowania lub jakiejkolwiek jej części oraz dokumentacji;

f) Wykonawca dostarczy Zamawiającemu jedynie kod wynikowy Oprogramowania;

g) Wykonawca nie jest uprawniony do wypowiedzenia licencji na podstawie art. 68 ust.1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

8.2. Wykonawca oświadcza i gwarantuje, że w przypadku Oprogramowania, którego nie jest Producentem oraz dokumentacji uzyskał zgodę Producenta na korzystanie z Oprogramowania i dokumentacji, niniejszym udziela licencji na warunkach określonych przez producenta i ust. 8.1 niniejszej umowy przekazując dokumenty określające warunki licencji.

8.3. Wykonawca oświadcza i gwarantuje, że Oprogramowanie i dokumentacja ani korzystanie z nich przez Zamawiającego zgodnie z Umową, nie będą naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich, patentów, ani praw do baz danych.

§ 9. ROSZCZENIA OSÓB TRZECICH

9.1 Wykonawca, z zastrzeżeniem poniższych postanowień, będzie występował, na własny koszt, w celu zażegnania sporu, w sprawie wszelkich roszczeń zgłoszonych wobec Zamawiającego w sądzie lub poza sądem, o ile takie roszczenia są związane z naruszeniem jakiegokolwiek prawa własności intelektualnej, w związku z używaniem przez Zamawiającego Oprogramowania , dostarczonego zgodnie z Umową. Wykonawca pokryje wszelkie odszkodowania oraz inne koszty ostatecznie zasądzone od Zamawiającego w związku z powyższym roszczeniem.

Wykonawca wstąpi do postępowania w charakterze strony pozwanej, a w razie braku takiej możliwości wystąpi z interwencją uboczną po stronie Zamawiającego.

9.2 Powyższe regulacje mają zastosowanie pod warunkiem, że Wykonawca:

- zostanie niezwłocznie powiadomiony przez Zamawiającego o takim roszczeniu;
- otrzyma pomoc w zakresie udostępnienia informacji i materiałów;
- osobie wskazanej przez Wykonawcę zostanie udzielone wyłączne pełnomocnictwo do obrony Zamawiającego przed takim roszczeniem.

9.3 Wykonawca ma obowiązek, na swój koszt, uzyskać dla Zamawiającego prawo do dalszego używania takiego Oprogramowania lub zastąpić takie Oprogramowanie innym oprogramowaniem, nienaruszającym powyższych praw, lub zmienić Oprogramowanie w taki sposób, że przestanie on naruszać powyższe prawa. Dostarczone oprogramowanie winno spełniać wymagania Zamawiającego w stopniu nie mniejszym, niż oprogramowanie podlegające wymianie. Wykonawca nie ponosi odpowiedzialności za żadne naruszenie praw własności intelektualnej, powstałe w wyniku używania Oprogramowania w sposób inny, niż określony w instrukcjach dostarczonych przez Wykonawcę, lub w wyniku używania Oprogramowania razem z towarami nie dostarczonymi przez Wykonawcę.

9.4 W odniesieniu do jakiegokolwiek Oprogramowania dostarczonego na mocy Umowy, w celu dalszej sprzedaży, dzierżawy lub najmu, użytkownik końcowy, któremu Zamawiający dostarczył Oprogramowanie będzie miał prawa takie, jak określono powyżej, pod warunkiem, że spełni wymogi na nim ciążące określone w niniejszych warunkach licencyjnych.

9.5 Strony potwierdzają, że żadne z powyższych postanowień nie wyłącza możliwości dochodzenia przez Zamawiającego odszkodowania lub wykonania uprawnień na zasadach ogólnych kodeksu cywilnego lub wynikających z innych ustaw.

§ 10. KARY UMOWNE I ODSTĄPIENIE OD UMOWY

10.1. Zamawiający jest uprawniony do naliczania Wykonawcy kar umownych:

a) za opóźnienie w realizacji przedmiotu Umowy w wysokości 0,5% ceny brutto określonej w § 5 ust. 1 umowy za każdy dzień opóźnienia w realizacji przedmiotu umowy, zgodnie z § 2 ust. 2 umowy,

b) za opóźnienie w wykonywaniu obowiązków gwarancyjnych i wsparcia technicznego, określonych w ofercie Wykonawcy w wysokości 0,5% ceny brutto określonej w § 5 ust. 1, za każdy dzień opóźnienia, za każde naruszenie.

10.2. W przypadku niewykonania przedmiotu Umowy w ciągu 7 dni od terminu ustalonego w § 2 umowy, Zamawiający może odstąpić od Umowy bez wyznaczania dodatkowego terminu. Wykonawca w tym przypadku zapłaci Zamawiającemu karę umowną w wysokości 10% ceny brutto określonej w § 5 ust. 1 umowy.

10.3. Oświadczenie o odstąpieniu od umowy zostanie złożone w terminie 7 dni kalendarzowych od daty powzięcia przez Zamawiającego wiadomości o wystąpieniu okoliczności uzasadniającej odstąpienie.

a) Zamawiający może dochodzić odszkodowania uzupełniającego, jeżeli szkoda przewyższy wysokość kar umownych na zasadach ogólnych kodeksu cywilnego.

10.4. Wykonawca wyraża zgodę na potrącanie kary umownej z przysługującej ceny.

§ 11. ODPOWIEDZIALNOŚĆ

11.1. Z zastrzeżeniem sytuacji odmiennie uregulowanych przez bezwzględnie obowiązujące przepisy prawa polskiego, łączna i całkowita odpowiedzialność Wykonawcy za szkody niezależnie od ich rodzaju, charakteru i przyczyn powstania, ograniczona jest do strat rzeczywistych, do kwoty określonej w § 5 ust. 1 powyżej. Wykonawca nie ponosi odpowiedzialności z tytułu utraconych korzyści ani szkód pośrednich.

11.2. Wykonawca nie ponosi odpowiedzialności za szkody polegające na utracie danych, kosztach związanych z ich odtworzeniem oraz niemożnością korzystania z danych utraconych przez Zamawiającego. Obowiązek utrzymywania procedury odtwarzania utraconych lub zmienionych plików, danych lub programów spoczywa na Zamawiającym. Ograniczenia odpowiedzialności, o których mowa w punkcie 10.1 powyżej oraz punkcie niniejszym obowiązują bez względu na rodzaj, charakter i przyczynę odpowiedzialności.

11.3. Wykonawca nie ponosi odpowiedzialności z tytułu ewentualnego ujawnienia się wad prawnych oprogramowania osób trzecich.

§ 12. SIŁA WYŻSZA

12.1. Strony Umowy nie są odpowiedzialne za niewykonanie lub nienależyte wykonanie zobowiązań spowodowane działaniem siły wyższej. Przez siłę wyższą rozumie się wszelkie okoliczności nieprzewidziane przez Strony Umowy lub, jeśli przewidziane, będące poza ich wpływem, które całkowicie lub częściowo uniemożliwiają wypełnienie postanowień Umowy. Siłę wyższą stanowią w szczególności klęski żywiołowe, pożary, powodzie, eksplozje, strajki, zamieszki, wojna (lista nie jest pełna ani zamknięta).

12.2. W przypadku działania siły wyższej ustalony okres czasu przeznaczony na wypełnienie postanowień Umowy zostanie przedłużony o czas działania siły wyższej. Gdyby ten okres przekraczał sześć tygodni, umawiające się Strony podejmą decyzję w sprawie dalszych zasad realizacji Umowy.

§ 13. POUFNOŚĆ

13.1. Każda ze Stron Umowy w okresie jej obowiązywania będzie chronić informacje pochodzące od drugiej Strony, które są określone jako poufne, w taki sam sposób, w jaki chroni i zabezpiecza swoje informacje poufne. Informacja poufna oznacza w szczególności jakąkolwiek informację lub dane uzyskane w okresie obowiązywania Umowy nie ujawnione wcześniej do publicznej wiadomości i dotyczące:

a) jednej ze Stron Umowy lub prowadzonej przez nią działalności;

b) klientów i produktów, struktury organizacyjnej, tajemnicy służbowej oraz informacji podlegających Ustawie o ochronie danych osobowych;

c) przedmiotu i zakresu Umowy i sposobu jej wykonywania;

d) objęte tajemnicą przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

13.2. Powyższe obowiązki poufności nie obejmują informacji przekazywanych przez Strony w ramach grupy kapitałowej (w rozumieniu przepisów ustawy z dnia 15 grudnia 2000 r. o ochronie konkurencji i konsumentów, Dz.U. z 2003 r. nr 86, poz. 804), podwykonawcom i doradcom oraz dla celów audytu.

13.3. Żadna ze Stron Umowy nie może domagać się traktowania jako poufnej informacji, którą druga ze Stron już posiada, które są publicznie znane, które zostały przez drugą Stronę niezależnie wypracowane lub które uzyskała ona zgodnie z prawem i bez klauzuli zachowania tajemnicy handlowej od osób trzecich, jak też informacje, których ujawnienie wymagane jest przez bezwzględnie obowiązujące przepisy prawa.

§ 14. POSTANOWIENIA KOŃCOWE

14.1. W przypadku sprzeczności pomiędzy postanowieniami części głównej Umowy a postanowieniami Załączników rozstrzygające będą postanowienia części głównej Umowy.

14.2. Wszelkie spory wynikające z niniejszej Umowy będą rozwiązywane przez Strony w miarę możliwości na drodze polubownej.

14.3. Jeżeli dany spór nie zostanie polubownie rozwiązany w ciągu 45 Dni roboczych od dnia, gdy jedna ze Stron przesłała drugiej pismo wszczynające spór, każda ze Stron może poddać spór rozstrzygnięciu sądu właściwego dla siedziby Zamawiającego

14.4. Jeżeli okaże się, że import niektórych Produktów wymaga uzyskania właściwych zezwoleń (licencji) importowych lub eksportowych, Zamawiający będzie współpracował z Wykonawcą w celu uzyskania wymaganych zezwoleń. Czas trwania stosownej procedury zawiesza bieg terminu dostawy.

14.5. Wykonawca uprawniony jest do wyboru wykwalifikowanych podwykonawców w ramach niniejszej Umowy. Za ich działania i zaniechania Wykonawca odpowiada, jak swoje własne działania lub zaniechania.

14.6. We wszystkich kwestiach nieuregulowanych niniejszą Umową stosuje się odpowiednie przepisy kodeksu cywilnego. Niniejsza Umowa wraz z jej Załącznikami stanowi całość porozumienia między Stronami i zastępuje wszelkie uprzednie i równoczesne porozumienia lub oświadczenia, czy to pisemne czy ustne, odnośnie przedmiotu Umowy Niniejsza Umowa, jak również jej Załączniki mogą zostać zmienione lub aneksowane wyłącznie w formie pisemnej, pod rygorem nieważności.

14.7. Niniejsza Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednej dla każdej ze Stron.

§ 15. ZAŁĄCZNIKI

Integralną część Umowy stanowić będzie następujący załącznik przygotowany przez Wykonawcę:

Załącznik 1 - Wykaz produktów (wykaz sprzętu, zakres gwarancji i wsparcia technicznego).

Zamawiający	Wykonawca

Załącznik 1

Wykaz produktów (wykaz sprzętu, zakres gwarancji i wsparcia technicznego).
