Wojewódzki Szpital Specjalistyczny w Legnicy

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA
W POSTĘPOWANIU O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO
W TRYBIE PODSTAWOWYM Z MOŻLIWOŚCIĄ NEGOCJACJI
NA DOSTAWĘ ASORTYMENTU MAJĄCEGO PODNIEŚĆ OCHRONĘ W ZAKRESIE CYBERBEZPIECZEŃSTWA

znak sprawy WSzSL/FZ-69/23

postępowanie przeprowadzane jest zgodnie z ustawą z dnia 11 września 2019 r.,

Prawo zamówień publicznych (t.j. Dz.U. z 2023 r. poz.1605 ze zm.)

Legnica, 25-09-2023r.

Rozdział I. Nazwa i adres Zamawiającego

Zamawiającym jest:
Wojewódzki Szpital Specjalistyczny w Legnicy
59-220 Legnica
ul. Iwaszkiewicza 5
NIP 691-22-04-853
tel. 76/ 72-11-142; 76/72-11-242
Strona internetowa prowadzonego postępowania:
https://platformazakupowa.pl/pn/szpital_legnica
Adres poczty elektronicznej: zam.publiczne@szpital.legnica.pl,
NIP 691-22-04-853, Województwo: dolnośląskie

Rozdział II. Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści specyfikacji warunków zamówienia oraz inne dokumenty związane z postępowaniem o udzielenie zamówienia

Zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej https://platformazakupowa.pl/pn/szpital_legnica

Rozdział III. Tryb udzielenia zamówienia

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, na podstawie art. 275 pkt 2 ustawy z dnia 11-09-2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2023 r., poz. 1605 ze zm.) oraz aktów wykonawczych wydanych na jej podstawie.
2. Użyte w niniejszej Specyfikacji Warunków Zamówienia (oraz w Załącznikach) terminy mają następujące znaczenie:
a) „uPzp" – ustawa z dnia 11-09-2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2023 r., poz. 1605 ze zm.)
b) „SWZ" – niniejsza Specyfikacja Warunków Zamówienia,
c) „zamówienie" – zamówienie publiczne, którego przedmiot został opisany w Rozdziale V niniejszej SWZ,
d) „postępowanie" – postępowanie o udzielenie zamówienia publicznego, którego dotyczy niniejsza SWZ,
e) „Zamawiający" – Wojewódzki Szpital Specjalistyczny w Legnicy,
f) „KSC"- ustawa z dnia 05.07.2018 o krajowym systemie cyberbezpieczeństwa,
g) „Zarządzenie" - Zarządzenie nr 108/2023/DI Prezesa Narodowego Fundusz Zdrowia z dnia 14 lipca 2023 r. zmieniające zarządzenie w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców,
h) „Umowa o dodatkowe finansowanie" - umowa z dnia 31-08-2023 r. Nr 01.3301161.42.D.2023 zawarta pomiędzy Narodowym Funduszem Zdrowia a Wojewódzkim Szpitalem Specjalistycznym w Legnicy w sprawie dodatkowego finansowania ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 działań w celu podniesienia poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców.
3. Wykonawca powinien dokładnie zapoznać się z niniejszą SWZ i złożyć ofertę zgodnie z jej postanowieniami.
4. Ilekroć w treści niniejszej SWZ wskazano akty prawne należy przyjąć, że zostały one przywołane w brzmieniu aktualnym na dzień wszczęcia przedmiotowego postępowania.

Rozdział IV. Informacja czy Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji

Zamawiający:
1) przewiduje możliwość prowadzenia negocjacji z Wykonawcami w celu ulepszenia treści ofert, które podlegają ocenie w ramach kryteriów oceny ofert.
2) nie przewiduje możliwości ograniczenia liczby Wykonawców, których zaprosi do negocjacji.

Rozdział V. Opis przedmiotu zamówienia

Nazwy i kody według Wspólnego Słownika Zamówień:

32420000-3 - Urządzenia sieciowe
48822000-6 Serwery komputerowe
48219500-1 - Pakiety oprogramowania do switcha lub routera
48781000-6 - Pakiety oprogramowania do zarządzania systemem
48223000-7 - Pakiety oprogramowania do poczty elektronicznej

1. Przedmiotem umowy jest wykonanie dostawy niżej wymienionych urządzeń i dostępnych na rynku oprogramowani w celu podniesienia cyberbezpieczeństwa Zamawiającego:
1) jednej sztuki biblioteki taśmowej oraz czterdziestu taśm,
2) jednej sztuki serwera,

3) jednej sztuki urządzenia UTM do rozbudowy istniejącego u Zamawiającego firewall,
4) systemu centralnego logowania, raportowania i korelacji,
5) systemu ochrony poczty elektronicznej
6) systemu uwierzytelniania, autoryzacji i kontroli dostępu,
- szczegółowo opisanych w Rozdziale XXVI SWZ.
2. Warunki dotyczące wykonywania zamówienia określone zostały również w projekcie umowy w Rozdziale VII SWZ.
3. Szczegółowy opis Przedmiotu zamówienia znajduje się w Rozdziale XXVI SWZ, który stanowić będzie Załącznik nr 1 do Umowy.
4. Opis przedmiotu zamówienia należy odczytywać wraz z ewentualnymi zmianami treści specyfikacji, będącymi np. wynikiem udzielonych odpowiedzi na zapytania Wykonawców.

Rozdział VI. Termin wykonania zamówienia

Wykonawca zobowiązany jest zrealizować przedmiot zamówienia w terminie do **dnia 20-10-2023 r.**

Rozdział VII. Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy

UMOWA Nr …...../FZ-69/23

zawarta w dniu …….w Legnicy pomiędzy: (dotyczy podpisywania umowy w sposób tradycyjny - na papierze)

zawarta w dniu złożenia podpisu przez ostatnią ze stron pomiędzy: (dotyczy umów podpisywanych w formie elektronicznej):

Wojewódzkim Szpitalem Specjalistycznym w Legnicy Samodzielnym Publicznym Zakładem Opieki Zdrowotnej z siedzibą w Legnicy, przy ul. J. Iwaszkiewicza 5 wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej Krajowego Rejestru Sądowego pod numerem 0000163872, którego akta rejestrowe przechowywane są przez Sąd Rejonowy dla Wrocławia-Fabrycznej IX Wydział Gospodarczy oraz wpisanym do rejestru podmiotów wykonujących działalność leczniczą prowadzonego przez Wojewodę Dolnośląskiego pod nr 000000001953

reprezentowanym przez:
…….. – …….
przy kontrasygnacie
….....-.....…
NIP 691-22-04-853
Regon 390999441

zwanym w dalszej części umowy Zamawiającym
a
.....
z siedzibą w
NIP
Regon

reprezentowanym przez:
….....
zwanym w dalszej części umowy Wykonawcą

Niniejsza umowa jest następstwem wyboru przez Zamawiającego oferty Wykonawcy w trybie podstawowym z możliwością przeprowadzenia negocjacji zgodnie ustawą z dnia 11-09-2021 r., Prawo zamówień publicznych (Znak WSzSL/FZ-69/23)

Przyjmuje się, że do użytej w niniejszej umowie terminologii zastosowanie mają zapisy Rozdziału **III SWZ**

§1

1. Przedmiotem umowy jest wykonanie dostawy niżej wymienionych urządzeń i dostępnych na rynku oprogramowani w celu podniesienia cyberbezpieczeństwa Zamawiającego:
1) jednej sztuki biblioteki taśmowej oraz czterdziestu taśm,
2) jednej sztuki serwera oraz
3) jednej sztuki urządzenia UTM do rozbudowy istniejącego u Zamawiającego firewall,
(zwanych dalej również: sprzętem)
4) systemu centralnego logowania, raportowania i korelacji,
5) systemu ochrony poczty elektronicznej oraz
6) systemu uwierzytelniania, autoryzacji i kontroli dostępu,
(zwanych dalej róweż: systemami)
- szczegółowo opisanych w Załączniku nr 1 do umowy (będącego odpowiednikiem Rozdziału XXVI SWZ).

2. Dostawa, o której mowa:
1) w ust. 1 pkt 1 obejmuje również dokonanie instalacji dostarczonego urządzenia w miejscu wskazanym przez Zamawiającego w jego siedzibie, konfiguracji dostarczonego urządzenia oraz połączenia go z urządzeniem, o którym mowa w ust. 1 pkt 2,
2) w ust. 1 pkt 2 obejmuje również dokonanie instalacji dostarczonego urządzenia w miejscu wskazanym przez Zamawiającego w jego siedzibie, instalacji i konfiguracji systemu operacyjnego, systemu backup Veeam (stanowiącego własność Zamawiającego) na dostarczonym urządzeniu oraz instalacji i konfiguracji na dostarczonym urządzeniu oraz konfigurację polityk backupu i weryfikację poprawności działania urządzenia,
3) w ust. 1 pkt 3 obejmuje również dokonanie rejestracji, konfiguracji dostarczonego urządzenia i jego oprogramowania , a także dokonanie aktualizacji oprogramowania, którego aktualnie używa Zamawiający a także stworzenie klastra z dostarczonego urządzenia z używanym aktualnie przez Zamawiającego (i stanowiącym jego własność) urządzeniem - FortiGate 101F,
4) w ust. 1 pkt 4 obejmuje również dokonanie rejestracji i instalacji systemu w środowisku informatycznym Zamawiającego, dokonanie konfiguracji warstwy sieciowej i ustawień systemowych Zamawiającego – mających na celu prawidłowe działanie dostarczonego systemu oraz połączenie klastra firewall i systemu ochrony poczty elektronicznej do zbierania logów,
5) w ust. 1 pkt 5 obejmuje również dokonanie rejestracji i instalacji systemu w środowisku informatycznym Zamawiającego, dokonanie konfiguracji: warstwy sieciowej, ustawień systemowych, profilów bezpieczeństwa, funkcji Sandbox, rekonstrukcji zawartości, nagłówków tematów [np.(Zew)] Zamawiającego, dokonanie integracji z aktualnie używanym przez Zamawiającego systemem poczty elektronicznej, skonfigurowanie logowania do systemu centralnego logowania, raportowania i korelacji, a także rekonfigurację rekordów MX w DNS;
6) w ust. 1 pkt 6 obejmuje również dokonanie rejestracji systemu, instalacji maszyny systemu na wirtualizatorze, konfiguracji dostępów (adresacja IP, dostęp administracyjny) oraz rejestracji i instalacji serwisów , aktywacji tokenów i konfiguracji 2FA dla dostępu VPN.
2. Przedmiot umowy w zakresie związanym z dostawą sprzętu obejmuje również:
1) jego rozładunek, wniesienie do miejsca montażu oraz przekazanie Zamawiającemu jego szczegółowej specyfikacji technicznej.
2) zapewnienie wszystkich niezbędnych kabli sygnałowych, złącz, przejściówek itp. koniecznych do prawidłowego podłączenia i uruchomienia dostarczonego sprzętu.
3. Wykonawca zobowiązuje się do wykonania Przedmiotu Umowy zgodnie z: opisem przedmiotu zamówienia znajdującym się w Załączniku nr 1 do umowy, obowiązującymi przepisami, KSC, Zarządzeniem, niniejszą umową, SWZ oraz najlepszą wiedzą w tym zakresie i ustaleniami z Zamawiającym, przy czym przedmiot zamówienia opisany w §1 ust. 2 pkt 1 i 2 zostanie wykonany przez inżyniera posiadającego aktualny certyfikat techniczny Veeam Certified Engineer (VMCE) i/lub Veeam Certified Architect (VMCA) oraz VMwarew vSphere VCP – co związane jest z faktem wykonania zamówienia w związku z oprogramowaniami, których właścicielem jest Zamawiający, a które będą instalowane przez Wykonawcę.
4. Dla interpretacji postanowień Umowy, w tym przede wszystkim dla określenia wzajemnych praw i obowiązków Stron dokumenty przywołane w Rozdziale III SWZ będą miały charakter wzajemnie uzupełniający, przy czym w razie kolizji pierwszeństwo mieć będą postanowienia tych dokumentów. Jednocześnie Strony postanawiają, iż dokumenty te będą wzajemnie wyjaśniające i uzupełniające, w tym znaczeniu, że w przypadku zaistnienia jakiejkolwiek niejednoznaczności, wieloznaczności lub rozbieżności, Strony nie ograniczą w żaden sposób ani Przedmiotu Umowy, ani zakresu należytej staranności.

§2

1.Wykonawca oświadcza, że przedmiot umowy:
1) w zakresie sprzętu pochodzi z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, jest wyprodukowany nie wcześniej niż 6 miesięcy przed dostawą ,fabrycznie nowy, nieużywany i niestanowiący przedmiotu demonstracji, pokazów, etc. i dostarczony będzie wraz z instrukcją obsługi, licencjami do zainstalowanych na nim oprogramowań, certyfikatami producenta, kartami gwarancyjnymi producenta.
2) w zakresie systemów dostarczone oprogramowanie jest najwyższej jakości, wolne od jakichkolwiek wad fizycznych lub prawnych i dostarczone będzie wraz z instrukcją obsługi, licencjami, certyfikatami producenta, kartami gwarancyjnymi producenta.
2. Wykonawca zwalnia Zamawiającego od wszelkiej odpowiedzialności w przypadku jakichkolwiek roszczeń osób trzecich dotyczących Przedmiotu Umowy.
3. W przypadku jakichkolwiek roszczeń osób trzecich zgłoszonych wobec Zamawiającego sądownie lub poza sądownie, o ile takie roszczenia są związane z naruszeniem praw osób trzecich w związku z realizacją Przedmiotu Umowy, Wykonawca podejmie na swój koszt wszelkie działania w celu rozwiązania takiego sporu, łącznie z prowadzeniem postępowania sądowego.
W takim przypadku Wykonawca zobowiązany jest do naprawienia wszelkich strat powstałych po stronie Zamawiającego z tego tytułu, w szczególności do pokrycia wszelkich odszkodowań oraz innych kosztów wynikających z tego tytułu. Powyższe zobowiązanie dotyczy również sytuacji zaistniałych mimo odstąpienia od Umowy.
4. Wykonawca oświadcza, że Przedmiot Umowy będzie wykonany z należytą starannością i na poziomie wymaganym od profesjonalnego dostawcy i usługodawcy.
5. Wykonawca ponosi pełną i wyłączną odpowiedzialność za działania lub zaniechania podmiotów, którym powierzył Przedmiot Umowy do realizacji w części, jak za własne działania lub zaniechania

§ 3

Przedmiot umowy wykonany zostanie w terminie do dnia 20-10-2023 r.

§ 3A

1. Dokumentem potwierdzającym prawidłowe wykonanie przedmiotu umowy będzie protokół odbioru. Protokół odbioru stanowić

będzie potwierdzenie należytego wykonania Umowy i stanowi podstawę do wystawienia faktury VAT.
2. Wykonawca dostarczy Zamawiającemu sprzęt i systemy na własny koszt i zgodnie z warunkami określonymi w umowie i poniesie pełne ryzyko związane z niebezpieczeństwem jego utraty albo uszkodzenia do chwili dokonania jego odbioru potwierdzonego podpisaniem protokołu odbioru, o którym mowa w ust. poprzedzającym.
3. W przypadku stwierdzenia braków lub wad w Wykonawca zobowiązuje się w terminie do 3 dni roboczych do usunięcia wad i dostarczenia rozwiązania bez wad, bez prawa do odrębnego wynagrodzenia z tego tytułu. Termin, o którym mowa w zdaniu poprzedzającym, liczony będzie od dnia przekazania Wykonawcy Protokołu z zastrzeżeniami drogą mailową na adres ……. . Ta sama procedura postępowania dotyczy stwierdzenia braków, wad lub nieprawidłowości w zakresie umownych obowiązków opisanych w Załączniku nr 1 do Umowy.
4. W przypadku nie usunięcia braków, wad lub nieprawidłowości przez Wykonawcę zgodnie z postanowieniami ust. 3 powyżej, Zamawiający ma prawo odstąpić od Umowy w terminie 30 (trzydziestu) dni kalendarzowych od bezskutecznego upływu terminu, o którym mowa w ust. e oraz naliczyć Wykonawcy kary umowne.
5. Jeżeli Zamawiający, mimo uwag lub zastrzeżeń, przyjmie Przedmiot Umowy, wówczas wynagrodzenie może ulec obniżeniu proporcjonalnie do zakresu wadliwości Przedmiotu Umowy.
6. Osobą wyznaczoną do kontaktów z Wykonawcą w sprawie realizacji niniejszej umowy oraz reklamacji jest ……..., tel. 76 72 -11-……...

§4

1. Wykonawca oświadcza, że dostarczone wraz z zamówionym sprzętem oprogramowanie zawiera niezbędny klucz licencyjny, licencja zaś odpowiada tej udzielonej przez producenta oprogramowania i jest bezterminowa. Wykonawca gwarantuje, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich i Wykonawca ponosi z tego tytułu pełną odpowiedzialność. Ponadto Zamawiający zastrzega sobie prawo weryfikacji czy dostarczony asortyment, oprogramowanie i powiązane z nimi elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem. W powyższym celu Zamawiający może zwrócić się do przedstawicieli producenta danego oprogramowania z prośbą o weryfikację czy oferowane oprogramowanie i materiały do niego dołączone są oryginalne. W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiet producenta, Zamawiający zastrzega sobie prawo do odstąpienia od umowy w terminie 30 dni od daty powzięcia takiej informacji . Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań.
2. Wykonawca oświadcza również, że będzie ponosił pełną odpowiedzialność z tytułu naruszenia praw osób trzecich w związku z realizacja dostawy sprzętu i udzieleniem licencji na oprogramowanie.
3. W ramach wynagrodzenia, o którym mowa w §5 ust. 1 Wykonawca, z chwilą podpisania protokołu, o którym mowa w §3A ust. 1, udziela Zamawiającemu bezterminowych licencji lub sublicencji na oprogramowanie lub zapewnia udzielenie bezterminowych licencji na oprogramowanie.

§ 5

1. Strony ustalają, że łączne wynagrodzenie należne z tytułu realizacji całego Przedmiotu Umowy wyniesie netto ….....zł powiększone o należny podatek VAT …… %, tj. łącznie wynagrodzenie brutto wyniesie …..... zł, w tym:
1) wynagrodzenie w zakresie określonym w § 1 ust. 1 pkt 1 ……. zł netto
2) wynagrodzenie w zakresie określonym w § 1 ust. 1 pkt 2 ……. zł netto
3) wynagrodzenie w zakresie określonym w § 1 ust. 1 pkt 3 ……. zł netto
4) wynagrodzenie w zakresie określonym w § 1 ust. 1 pkt 4 ……. zł netto
5) wynagrodzenie w zakresie określonym w § 1 ust. 1 pkt 5 ……. zł netto
6) wynagrodzenie w zakresie określonym w § 1 ust. 1 pkt 6 ……. zł netto
2. Zapłata będzie zrealizowana przelewem bankowym na konto Wykonawcy w terminie 60 dni liczonym od dnia otrzymania prawidłowo wystawionej faktury, sporządzonej w oparciu o Protokół, o którym mowa w §3A ust. 1.
3. Faktura winna być złożona Zamawiającemu lub dostarczona w sposób określony w ust. 4 wraz z protokołem, nie później jednak niż do **20-10-2023 r.**
4. Wykonawca ma prawo przesyłać Zamawiającemu ustrukturyzowane faktury elektroniczne za pośrednictwem Platformy Elektronicznego Fakturowania https://www.brokerinfinite.efaktura.gov.pl/ Skrzynka: Wojewódzki Szpital Specjalistyczny w Legnicy, adres: Jarosława Iwaszkiewicza 5, 59-220 Legnica, dane identyfikacyjne skrzynki – nr PEPPOL 6912204853; skrócona nazwa skrzynki: WSzS w Legnicy

§5A

1. Zamawiający oświadcza, że będzie realizować płatności za fakturę/y z zastosowaniem mechanizmu podzielonej płatności tzw. split payment.
2. Zapłatę w tym systemie uznaje się za dokonanie płatności w terminie ustalonym w §5 ust. 2 umowy
3. Podzieloną płatność tzw. split payment stosuje się wyłącznie przy płatnościach bezgotówkowych, realizowanych za pośrednictwem polecenia przelewu lub polecenia zapłaty dla czynnych podatników VAT.
4. 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% lub objęte odwrotnym obciążeniem.
5. Wykonawca oświadcza, że wyraża zgodę na dokonywanie przez Zamawiającego płatności w systemie podzielonej płatności tzw. split payment.

6. Wykonawca oświadcza, że numer rachunku rozliczeniowego wskazany we wszystkich fakturach, stanowiących podstawę płatności za wykonanie umowy, jest rachunkiem dla którego prowadzony jest rachunek VAT zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - Prawo Bankowe.

§6

1. Okres udzielonej przez Wykonawcę gwarancji dla sprzętu wskazany jest w Załączniku nr 1 do umowy. Bieg okresu gwarancji rozpoczyna się następnego dnia po dacie podpisania protokołu odbioru, o którym mowa w §3A ust. 1 umowy. Zamawiający może dochodzić roszczeń z tytułu gwarancji także po upływie terminu o którym mowa w zdaniu pierwszym, jeżeli zgłosił wadę przed jego upływem - w takim przypadku roszczenia Zamawiającego wygasają w ciągu roku od dnia zgłoszenia wady.
2. Wykonawca zapewni możliwość zgłaszania wad i awarii przedmiotu zakupu, telefonicznie oraz drogą mailową Zgłoszenia będą dokonywane pod nr tel. …… lub na adres poczty elektronicznej ……..; zgłoszenie telefoniczne powinno być potwierdzone mailem.
3. Wykonawca potwierdzi przyjęcie zgłoszenia wady i/lub awarii na adres poczty elektronicznej, z którego zostało wysłane zgłoszenie.
4. Wykonawca zobowiązuje się do podjęcia czynności mających na celu usunięcie wady na następny dzień roboczy od momentu zgłoszenia, niezależnie od faktu potwierdzenia, bądź też nie potwierdzenia przez Wykonawcę otrzymania zgłoszenia zgodnie z ust. 3, z tym zastrzeżeniem, że wiadomość, w przypadku wysłania jej bądź zgłoszenie telefoniczne dokonane między godz. 8.00 a 16.00 w danym dniu roboczym uznana/uznane jest za doręczoną/zgłoszone w tym dniu roboczym, natomiast w przypadku jej wysłania po godz. 16.00 lub w dniu nie będącym dniem roboczym, uznana/uznane jest za doręczoną/ zgłoszone w następnym dniu roboczym
W przypadku zgłoszenia wady Wykonawca jest zobowiązany do jej niezwłocznego usunięcia, nie później jednak niż:
a) w terminie **siedmiu** dni roboczych liczonym od upływu terminu określonego w zdaniu pierwszym niniejszego ustępu - w przypadku, gdy wada uniemożliwia użytkowanie przedmiotu gwarancji,
b) w terminie **czternastu** dni roboczych liczonym od upływu terminu określonego w zdaniu pierwszym niniejszego ustępu - w pozostałych przypadkach;
5. Wykonawca oświadcza i gwarantuje, iż serwis gwarancyjny będzie realizowany przez producenta lub autoryzowanego partnera serwisowego producenta;
6. Serwis gwarancyjny dla sprzętu świadczony będzie w miejscu użytkowania sprzętu.
7. Koszt dojazdu serwisu w ramach napraw gwarancyjnych jak i koszty transportu przedmiotu umowy naprawianego w ramach gwarancji poza siedzibą Zamawiającego, pokrywa Wykonawca.
8. W przypadku awarii sprzętu, która nie została usunięta w terminie 30 dni od dnia zgłoszenia lub wystąpienia konieczności dwukrotnego usunięcia tej samej wady zarówno w zakresie naprawy, jak i wymiany (części, elementu, podzespołu, itp.), Wykonawca zobowiązuje się do bezzwłocznej wymiany urządzeń na fabrycznie nowe o parametrach nie gorszych aniżeli wynikające z umowy oraz oferty Wykonawcy.
9. Wymagana jest dostępność części zamiennych przez min. 5 lat liczonych od dnia podpisania protokołu, o którym mowa §3A ust. 1.
10.Niezależnie od udzielonej gwarancji Wykonawca ponosi odpowiedzialność z tytułu rękojmi na zasadach ogólnych z tym zastrzeżeniem, że strony rozszerzają rękojmię w ten sposób, że w przypadkach gdy okres rękojmi określony w przepisach prawa jest krótszy niż okres udzielonej przez Wykonawcę gwarancji, okres rękojmi przedłuża się na okres udzielonej gwarancji.
11. W przypadku wystąpienia awarii dysku twardego w sprzęcie, o którym mowa w § 1 ust. 1 pkt 2, uszkodzony dysk twardy pozostaje u Zamawiającego.

§7

1. Wykonawca zapłaci Zamawiającemu kary umowne:
1) w przypadku niewykonania przez Wykonawcę Przedmiotu Umowy w terminie określonym w §3, Wykonawca zapłaci Zamawiającemu karę umowną za każdy dzień opóźnienia w wysokości 1 % łącznej wartości netto określonej w §5 ust. 1. Taka sama kara będzie przysługiwać Zamawiającemu za każdy dzień zwłoki w usunięciu zgłoszonych wad/usterek w stosunku do ustalonych terminów ich usunięcia;
2) w przypadku uchybienia terminowi wskazanemu w §5 ust. 3 Wykonawca zapłaci Zamawiającemu karę umowną za każdy dzień opóźnienia w wysokości 0,7 % łącznej wartości netto określonej w §5 ust. 1.
3) w przypadku odstąpienia przez Wykonawcę od realizacji niniejszej umowy, z przyczyn nie leżących po stronie Zamawiającego, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10 % łącznej wartości netto Przedmiotu Umowy określonej w §5 ust. 1;
4) w przypadku odstąpienia od Umowy przez Zamawiającego, jeśli nastąpi ono z winy Wykonawcy, Wykonawca zobowiązany jest do zapłaty Zamawiającemu kary umownej w wysokości 10% wartości netto Przedmiotu Umowy określonej w § 5 ust. 1;
2. W przypadku naruszenia zasad ochrony danych osobowych lub zasad poufności przez Wykonawcę, Zamawiający może naliczyć karę umowną w wysokości 10 000 zł brutto, za każdy przypadek naruszenia.
3. Zamawiający zapłaci Wykonawcy karę umowną w wysokości 10 % wartości netto Przedmiotu Umowy określonej w §5 ust. 1 w przypadku odstąpienia od realizacji niniejszej umowy przez Wykonawcę, jeśli nastąpi ono z winy Zamawiającego.
4. Strony mogą dochodzić na zasadach ogólnych odszkodowania przewyższającego wszelkie zastrzeżone w niniejszej umowie kary umowne, do wysokości faktycznie poniesionej szkody z wyłączeniem utraconych korzyści.
5. Zamawiający zastrzega sobie prawo do potrącenia wierzytelności z tytułu naliczonych kar umownych z należności Zamawiającego wobec Wykonawcy choćby były one jeszcze niewymagalne.
6. Łączna maksymalna wysokość kar umownych naliczonych Wykonawcy nie może przekroczyć 20% łącznej wartości wynagrodzenia netto określonego w §5 ust. 1.
7. Zapłata kar umownych nie zwalnia Wykonawcy od obowiązku należytego wykonania Przedmiotu Umowy.

§8

1. Umowa może zostać zmieniona w sytuacji gdy:
1) zaistnieją nadzwyczajne okoliczności, których Zamawiający działając z należytą starannością nie mógł przewidzieć, powodujące że realizacja Umowy w sposób i w zakresie określonym pierwotnie w Umowie nie leży w interesie publicznym;
2) nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację Umowy;
3) zaistnieje działanie siły wyższej rozumianej jako nadzwyczajne okoliczności niezależne od Stron, których nie można było przewidzieć, jak m.in.: wojna, stany wyjątkowe, strajki generalne, blokady, embargo, działania sił przyrody o charakterze klęsk żywiołowych jak huragany, powodzie, trzęsienia ziemi, pożary, epidemie, pandemie itp., uniemożliwiającej realizację w części lub w całości Przedmiotu Umowy;
2. Strony są uprawnione do zmiany Umowy w zakresie materiałów, parametrów technicznych, technologii, sposobu i zakresu wykonania Przedmiotu Umowy, w następujących sytuacjach:
1) konieczności zrealizowania jakiejkolwiek części Przedmiotu Umowy, przy zastosowaniu odmiennych rozwiązań technicznych lub technologicznych, niż wskazane w Załączniku nr 1 do umowy, a wynikających ze stwierdzonych wad w opisie przedmiotu zamówienia tam zawartym lub zmiany stanu prawnego w oparciu, o który je przygotowano, gdyby zastosowanie przewidzianych rozwiązań groziło niewykonaniem lub nienależytym wykonaniem Przedmiotu Umowy,
2) wystąpienia siły wyższej uniemożliwiającej wykonanie Przedmiotu Umowy zgodnie z jej postanowieniami.
3. W razie wątpliwości, przyjmuje się, że nie stanowią zmiany Umowy następujące zmiany:
1) danych związanych z obsługą administracyjno-organizacyjną Umowy,
2) danych teleadresowych,
3) danych rejestrowych,
4) będące następstwem sukcesji uniwersalnej po jednej ze stron Umowy.

§9

Wykonawca zobowiązuje się zachować w poufności wszelkie informacje techniczne, technologiczne, ekonomiczne, finansowe, handlowe, prawne, organizacyjne, informacje zawierające dane osobowe i dotyczące sposobów zabezpieczania danych osobowych, a ponadto informacje dotyczące stosowanych systemów informatycznych w tym systemów bezpieczeństwa i inne dotyczące drugiej Strony, otrzymane od drugiej Strony w związku z realizacją Umowy, wyrażone za pomocą mowy, pisma, obrazu, rysunku, znaku, dźwięku albo zawarte w urządzeniu, przyrządzie lub innym przedmiocie, a także wyrażone w jakikolwiek inny sposób i przekazane drugiej Stronie. Kwestie poufności reguluje **Umowa o zachowaniu poufności stanowiąca Załącznik nr 3 do niniejszej Umowy.**

§10

Powierzenie przetwarzania danych osobowych w celu realizacji niniejszej Umowy odbywa się na podstawie umowy powierzenia przetwarzania danych osobowych, która stanowi Załącznik nr 2 do Umowy.

§11

1. Zamawiającemu przysługuje prawo odstąpienia od Umowy jeżeli wystąpi istotna zmiana okoliczności powodująca, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy lub dalsze wykonywanie Umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu. Odstąpienie od Umowy w takim przypadku może nastąpić w terminie 30 dni od powzięcia informacji o powyższych okolicznościach. W takim przypadku odstąpienie od Umowy nie rodzi roszczeń odszkodowawczych ani nie stanowi podstawy do naliczania kar umownych.
2. Zamawiającemu przysługuje prawo odstąpienia od umowy w całości, bądź w części wg swojego wyboru w przypadku naruszenia przez Wykonawcę warunków niniejszej umowy, w tym w szczególności:
1) gdy Wykonawca nie wykonuje Przedmiotu Umowy lub też nienależycie wykonuje swoje zobowiązania umowne,
2) gdy dostarczony/wykonany przez Wykonawcę Przedmiot Umowy nie spełnia wymagań szczegółowo określonych w Załączniku nr 1,
3) gdy termin, o którym mowa w § 3 został przekroczony o 2 lub więcej dni kalendarzowych
4) w przypadku rażącego naruszenia przez Wykonawcę innych zobowiązań wynikających z Umowy, Umowy o zachowaniu poufności bądź Umowy o powierzenie przetwarzania danych osobowych;
5) w innych przypadkach określonych niniejszą umową lubumowami, o których mowa w pkt 4) powyżej, oraz na zasadach przewidzianych przepisami Kodeksu cywilnego.
3. Zamawiający może również odstąpić od Umowy w całości bądź w części, wg swojego wyboru, bez wyznaczania terminu dodatkowego, z zachowaniem prawa do odszkodowań i kar określonych Umową, jeżeli:
1) nastąpi likwidacja przedsiębiorstwa Wykonawcy;
2) zostanie zajęty majątek Wykonawcy uniemożliwiając mu prawidłowe w tym terminowe wykonanie Przedmiotu Umowy;
3) wystąpią inne okoliczności uniemożliwiające lub ograniczające prawidłowe wykonywanie przez Wykonawcę jego obowiązków wynikających z Umowy.
4. Odstąpienie od Umowy, o którym mowa w ust. 2 i 3 powyżej, może nastąpić w terminie 30 dni od powzięcia informacji o wystąpieniu przesłanki odstąpienia.
5. Odstąpienie od umowy winno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia i powinno zawierać uzasadnienie.

§ 12

– nie dotyczy Wykonawcy wykonującego Przedmiot zamówienia bez udziału Podwykonawców

1. Zlecenie wykonania części zamówienia podwykonawcom nie zmienia zobowiązań Wykonawcy wobec Zamawiającego za wykonanie tej części zamówienia.

2. Wykonawca jest odpowiedzialny za działania, uchybienia i zaniedbania podwykonawców i ich pracowników w takim samym stopniu, jakby to były jego własne działania, uchybienia lub zaniedbania.
3. Wykonawca w Załączniku nr 2 do niniejszej umowy wskazał podwykonawców którzy będą brali udział w realizacji przedmiotu umowy.
4. Zmiana podwykonawców (jeśli dotyczy) wskazanych w załączniku nr 2 do niniejszej mowy wymaga zgłoszenia tego faktu Zamawiającemu.

§ 13

Dopuszcza się zmianę umowy w zakresie wynagrodzenia w przypadku zmiany powszechnie obowiązujących przepisów prawa podatkowego w takim zakresie, aby w razie wzrostu obciążeń podatkowych (VAT i akcyza) nie uległa wzrostowi kwota netto wynagrodzenia, zaś w przypadku obniżenia należności podatkowych (VAT i akcyza) aby kwota brutto została zmniejszona o równowartość zmniejszenia należności podatkowych Wykonawcy.

§14

1. W ramach Wynagrodzenia, o którym mowa w §5 ust. 1 Umowy, Wykonawca przeniesie na Zamawiającego majątkowe prawa autorskie do wszelkich utworów oraz ich elementów składowych zgodnie z wymogami postawionymi w niniejszej Umowie i wytworzonych w wyniku realizacji niniejszej Umowy, których Wykonawca jest autorem i które będą dziełem w rozumieniu ustawy o prawie autorskim i prawach pokrewnych, na następujących polach eksploatacji:
1) stosowanie zgodnie z przeznaczeniem, wprowadzanie, wyświetlanie, przechowywanie niezależnie od formatu, systemu lub standardu,
2) trwałe lub czasowe utrwalanie lub zwielokrotnianie, jakimikolwiek środkami i w jakiejkolwiek formie, niezależnie od formatu, systemu lub standardu, w tym: techniką magnetyczną na dyskach audio, techniką cyfrową, zapisu magnetycznego i optycznego egzemplarzy utworu, techniką zapisu komputerowego, w sieci multimedialnej (w tym Internet), jak i przesyłu pomiędzy sieciami komputerowymi,
3) wprowadzanie na własny użytek do pamięci komputera i do sieci multimedialnej,
4) prawo do rozporządzania utworami oraz prawo udostępniania ich do korzystania, w tym udzielania licencji na rzecz osób trzecich, na wszystkich wymienionych powyżej polach eksploatacji.
2. Wykonawca zapewnia Zamawiającego, że w razie pojawienia się nowych pól eksploatacji, które nie są wymienione w ust. 1 powyżej, będzie mu przysługiwało prawo żądania od Wykonawcy skutecznego przeniesienia na Zamawiającego dalszych praw.
3. Wraz z przeniesieniem praw, o których mowa w ust. 1 powyżej, Wykonawca w ramach otrzymanego Wynagrodzenia, przenosi na Zamawiającego prawo do zezwalania na wykonywanie zależnych praw autorskich do utworu, którego Wykonawca jest autorem, oraz jego elementów składowych na polach eksploatacji wymienionych w ust. 1 powyżej.
4. W ramach wynagrodzenia określonego w § 5 ust. 1, Zamawiającemu przysługuje prawo do przeniesienia nabytych praw autorskich majątkowych na osoby trzecie bez zgody Wykonawcy, wprowadzania zmian w utworze, udzielania zezwoleń na rozporządzanie i korzystanie z opracowań utworu oraz wykonywania wszelkich zależnych praw autorskich.
5. Rozporządzanie i korzystanie z praw nabytych przez Zamawiającego nie jest ograniczone czasowo ani terytorialnie.
6. Przeniesienie całości autorskich praw majątkowych następuje w chwili wytworzenia utworu którego Wykonawca jest autorem, przekazania go Zamawiającemu i podpisania protokołu odbioru, również tą chwilą nastąpi również przeniesienie na Zamawiającego prawa własności do egzemplarzy, na których utwór został utrwalony.
7. Wykonawca oświadcza, że wykonany i dostarczony utwór autorstwa Wykonawcy będzie wolny od wad fizycznych i prawnych, Wykonawcy będą przysługiwały całościowe wyłączne majątkowe prawa autorskie, konieczne do przeniesienia tych praw na Zamawiającego oraz, że prawa te nie będą w żaden sposób ograniczone. Wykonawca oświadcza także, że rozporządzenie prawami autorskimi do dzieł których będzie autorem nie narusza żadnych praw własności przemysłowej i intelektualnej, w szczególności praw patentowych, praw autorskich i praw do znaków towarowych. Wykonawca ponosi wyłączną odpowiedzialność za wszelkie roszczenia osób trzecich z tytułu naruszenia przez niego cudzych praw autorskich, w związku z realizacją Przedmiotu Umowy a ponadto oświadcza, że zaspokoi wszelkie uzasadnione roszczenia, a w razie ich zasądzenia od Zamawiającego regresowo zwróci mu całość pokrytych roszczeń oraz wszelkie związane z tym wydatki i opłaty, włączając w to koszty procesu i obsługi prawnej.
8. Jeżeli utwór którego Wykonawca jest autorem, bądź też jego elementy składowe będą miały wady prawne, Wykonawca, zobowiązany będzie do dostarczenia w wyznaczonym przez Zamawiającego terminie elementów wolnych od wad.
9. Wykonawca zobowiązuje się do niewykonywania przysługujących mu autorskich praw osobistych do utworów mających powstać w toku realizacji niniejszej umowy - względem Zamawiającego i jego następców prawnych, na których zostaną przeniesione autorskie prawa majątkowe do utworu, będącego przedmiotem niniejszej umowy. Wykonawca upoważnia Zamawiającego do wykonywania tych praw, w szczególności do:
1) anonimowej publikacji utworu,
2) decydowania o rozpowszechnianiu utworu,
3) decydowania o sposobie, miejscu i terminie publikacji,
4) decydowania o podpisie pod utworem,
5) przeniesienia uprawnień (wszystkich lub niektórych) wynikających z niniejszej umowy dla Zamawiającego, na ewentualnego nabywcę autorskich praw majątkowych do utworu lub licencjobiorcę, w wypadku przeniesienia na niego tych praw przez Zamawiającego.

§ 15

Wszelkie zmiany i uzupełnienia niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§16

Strony zgodnie przyjmują, że w przypadku zobowiązań Zamawiającego wynikających z niniejszej umowy, czynność prawna mająca na celu zmianę wierzyciela może nastąpić wyłącznie w trybie określonym przepisami ustawy z dnia 15 kwietnia 2011 r. o

działalności leczniczej, to jest po wyrażeniu na to zgody przez podmiot tworzący Zamawiającego oraz po wyrażeniu na to zgody przez Zamawiającego, w formie pisemnej pod rygorem nieważności. W przypadku naruszenia przez Wykonawcę lub jakąkolwiek osobę trzecią przepisów ww. ustawy, Zamawiający może wystąpić do sądu o stwierdzenie nieważności takiej czynności prawnej.

§17

W sprawach nie uregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy prawa polskiego.

§18

1. Strony zobowiązane są do stosowania postanowień niniejszej umowy, jak również SWZ oraz złożonej oferty (*oferty dodatkowej**), na podstawie których umowa ta została zawarta, stąd wszelkie zmiany niniejszej umowy wymagają dla swej ważności formy pisemnej
2. Spory wynikłe na tle realizacji niniejszej umowy strony zobowiązują się rozwiązać polubownie, a w przypadku gdy okaże się to niemożliwe, przez sąd powszechny właściwy miejscowo dla Zamawiającego.
3.W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy prawa polskiego.

[4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach z przeznaczeniem po jednym dla każdej ze stron.] – *ustęp objęty kwadratowym nawiasem dotyczy umowy zawieranej w formie pisemnej na papierze.*

*- w przypadku, gdy dotyczy

ZAMAWIAJĄCY **WYKONAWCA**

Umowa o zachowaniu poufności

zawarta pomiędzy:

Wojewódzkim Szpitalem Specjalistycznym w Legnicy Samodzielnym Publicznym Zakładem Opieki Zdrowotnej z siedzibą w Legnicy, przy ul. J. Iwaszkiewicza 5 wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej Krajowego Rejestru Sądowego pod numerem 0000163872, którego akta rejestrowe przechowywane są przez Sąd Rejonowy dla Wrocławia-Fabrycznej IX Wydział Gospodarczy oraz wpisanym do rejestru podmiotów wykonujących działalność leczniczą prowadzonego przez Wojewodę Dolnośląskiego pod nr 000000001953
NUMER REJESTRU BDO : 000111603 NIP 691-22-04-853; Regon 390999441; reprezentowanym przez:
…….
Zwany dalej Szpitalem

a

[.....

zwany dalej **Wykonawcą**

Zważywszy, że Strony zawarły umowę nr ……../FZ - /23, w ramach której Wykonawca może otrzymać informacje dotyczące aktywów Szpitala, danych dotyczących infrastruktury informatycznej, stosowanych sposobów zabezpieczeń, a współpraca pomiędzy Stronami będzie wymagała przekazania Wykonawcy przez Szpital Informacji Poufnych (w znaczeniu zdefiniowanym poniżej), Strony postanawiają co następuje:

§1

1. Na potrzeby niniejszej umowy, zwanej dalą Umową jako Informacje Poufne traktowane będą wszelkie informacje ujawnione Wykonawcy na piśmie, ustnie, drogą elektroniczną lub w jakikolwiek inny sposób (w szczególności w formie prezentacji, rysunków, filmów, dokumentów), bezpośrednio lub pośrednio przez Szpital (jego pracowników lub współpracowników, doradców) lub podmioty powiązane ze Szpitalem kapitałowo/osobowo lub z nim współpracujące i działające na jego zlecenie, zarówno przed jak i po dniu zawarcia Umowy, w tym w szczególności (lecz nie wyłącznie):
   a. informacje techniczne, technologiczne, organizacyjne Szpitala lub podmiotów powiązanych z nim kapitałowo/osobowo, a także inne informacje posiadające wartość gospodarczą;
   b. informacje handlowe, finansowe, księgowe, osobowe (w tym w szczególności pacjentów oraz dotyczące pracowników i współpracowników) Szpitala bądź podmiotów powiązanych kapitałowo/osobowo ze Szpitalem lub z nim współpracujące, informacje dotyczące cen, planów handlowych, dostawców, informacje dotyczące klientów, potencjalnych klientów;
   c. informacje odnoszące się do kapitału intelektualnego Szpitala bądź podmiotów powiązanych kapitałowo/osobowo ze Szpitalem (w tym rozwiązań innowacyjnych oraz doświadczenia związanego z ich stosowaniem), know-how, dane techniczne;
   d. wszelkie inne informacje określone przez Szpital lub podmioty powiązane ze Szpitalem kapitałowo/osobowo jako poufne
2. Informacjami Poufnymi nie są informacje dostępne publicznie ani takie, wobec których Wykonawca może udowodnić, że były mu znane przed ich ujawnieniem przez Szpital bądź podmioty powiązane ze Szpitalem kapitałowo/osobowo lub z nim współpracujące.

3. W przypadku jakichkolwiek wątpliwości co do charakteru danej informacji, przed jej ujawnieniem bądź uczynieniem dostępną, Wykonawca zobowiązany jest zwrócić się do Szpitala o wskazanie, czy informację tę ma traktować jako Informację Poufną.

§2

1. Wykonawca zobowiązuje się wykorzystywać Informacje Poufne wyłącznie w celu realizacji umowy nr ……../FZ - /23
2. Przez okres 5 (pięć) lat od dnia zawarcia Umowy, Wykonawca zobowiązuje się utrzymać w poufności Informacje Poufne, w tym w szczególności:
   a. z zastrzeżeniem postanowień pkt. c poniżej, nie ujawniać ani nie przekazywać Informacji Poufnych, pośrednio ani bezpośrednio, osobom trzecim; za ujawnienie Informacji Poufnych w rozumieniu Umowy uważa się także zaniechanie zabezpieczenia przed dostępem osób trzecich;
   b. nie kopiować ani nie powielać Informacji Poufnych bez uprzedniej pisemnej zgody Szpitala, chyba że jest to niezbędne dla realizacji Projektu;
   c. ujawniać Informacje Poufne pracownikom lub współpracownikom tylko w takim zakresie, w jakim jest to niezbędne dla realizacji Umowy nr ….. i po uprzednim zobowiązaniu takich osób do zachowania poufności na poziomie co najmniej ustalonym Umową. Wykonawca ponosi pełną odpowiedzialność za niewykonanie lub nienależyte wykonanie obowiązku zachowania poufności Informacji Poufnych takich osób.
3. Z zastrzeżeniem wyłączeń określonych Umową ujawnienie lub rozpowszechnienie Informacji Poufnych wymaga każdorazowo uprzedniej pisemnej zgody Szpitala.
4. Wykonawca dołoży należytych starań w celu zapewnienia, aby środki łączności, wykorzystywane przez Wykonawcę do odbioru oraz przekazywania Informacji Poufnych a także systemy informatyczne oraz pomieszczenia, w których Informacje Poufne są przechowywane, gwarantowały zabezpieczenie Informacji Poufnych przed dostępem do nich osób nieupoważnionych.
5. W wypadku, gdy Wykonawca zostanie zobowiązany prawomocnym orzeczeniem sądu bądź organu administracji państwowej do ujawnienia Informacji Poufnych albo konieczność ich ujawnienia będzie wynikała z przepisów prawa, Wykonawca zobowiązuje się niezwłocznie, jeżeli będzie to prawnie dopuszczalne jeszcze przed ujawnieniem, pisemnie powiadomić o tym fakcie Szpital oraz poinformować odbiorcę Informacji Poufnych o ich poufnym charakterze.
6. Wykonawca zobowiązany jest niezwłocznie powiadomić Szpital na piśmie o każdym stwierdzonym przypadku ujawnienia Informacji Poufnych osobom nieupoważnionym (w tym także zagubienia, kradzieży lub nieuprawnionego zniszczenia nośników, dokumentów lub innych materiałów zawierających Informacje Poufne) oraz podjęcia wszelkich koniecznych czynności w celu zapobieżenia dalszemu ujawnianiu Informacji Poufnych.
7. Szpital nie ponosi odpowiedzialności za prawdziwość lub kompletność Informacji Poufnych oraz nie udziela jakichkolwiek zapewnień, ani wyraźnie ani w sposób dorozumiany co do jakości lub przydatności danej Informacji Poufnej.

§3

1. Za naruszenie przez Wykonawcę obowiązków określonych Umową zapłaci on Szpitalowi karę umowną w wysokości 20.000,00 zł. (dwadzieścia tysięcy złotych) za każde naruszenie.
2. Niezależenie od zastrzeżonej kary umownej, Szpital jest uprawniony do dochodzenia odszkodowania na zasadach ogólnych.

§4

1. Umowa zawarta jest w celu określenia zasad przekazywania przez Szpital Informacji Poufnych i ich utrzymywania w poufności przez Wykonawcę. Umowa nie stanowi umowy przedwstępnej lub jakiejkolwiek umowy zobowiązującej do świadczeń innych niż związanych z realizacją umowy, o której mowa w preambule Umowy.
2. Wykonawca gwarantuje, że wszelkie podmioty z nim powiązane osobowo lub kapitałowo zostaną przez niego zobowiązane do przestrzegania niniejszej Umowy, o ile ujawnienie im Informacji Poufnych będzie niezbędne do realizacji umowy ……../FZ -69 /23Wykonawca odpowiada jak za swoje działania lub zaniechania tych podmiotów.
3. Wszelkie materiały zawierające Informacje Poufne stanowią i pozostają własnością Szpitala.
4. Po zakończeniu obowiązywania Umowy, bądź na każde żądanie Szpitala, Wykonawca niezwłocznie zwróci Szpitalowi wszelkie materiały oraz ich kopie zawierające Informacje Poufne a także usunie wszelkie Informacje Poufne zapisane w jakimkolwiek urządzeniu lub na jakimkolwiek nośniku służącym do przechowywania danych, w sposób uniemożliwiający ich ponowne odtworzenie oraz potwierdzi pisemnie Szpitalowi wykonanie tych obowiązków.
5. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
6. Prawem właściwym dla Umowy jest prawo polskie.
7. Sądem właściwym dla spraw wynikłych z Umowy jest właściwy rzeczowo Sąd powszechny w Legnicy.
8. *Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej Strony.] – nie dotyczy umów zawieranych w formie elektronicznej*

ZAMAWIAJĄCY **WYKONAWCA**

Umowa powierzenia przetwarzania danych osobowych
(dalej również: „Umowa")

zawarta pomiędzy:
Wojewódzkim Szpitalem Specjalistycznym w Legnicy z siedzibą w Legnicy przy ul. Iwaszkiewicza 5 (kod pocztowy: 59-220), wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej prowadzonym przez Sąd Rejonowy dla Wrocławia-Fabrycznej we Wrocławiu, IX wydział gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000163872, NIP: 691-220-48-53, REGON: 390999441;

reprezentowanym przez:
……
(dalej również: „Powierzający")
a …….
reprezentowanym przez:
……
(dalej również: „Procesor")

(Powierzający i Procesor zwani są dalej łącznie „Stronami", a każdy z osobna „Stroną")

Mając na uwadze fakt, że Strony zawarły umowę Nr……../FZ-69 /23 na podstawie której Procesor zobowiązał się do przetwarzania danych osobowych (dalej również „Umowa Główna"), Strony zawierają Umowę o następującej treści:

§ 1
Przedmiot powierzenia i oświadczenia Stron

1. Powierzający oświadcza, że jest uprawniony do powierzenia przetwarzania danych osobowych w zakresie wskazanym w Załączniku nr 1 i na zasadach wskazanych w niniejszej Umowie powierza Procesorowi do przetwarzania dane osobowe.
2. Zakres powierzenia, wskazany w Załączniku nr 1, może zostać w każdym momencie rozszerzony albo ograniczony przez Powierzającego. Zmiana Załącznika nr 1 w zakresie ograniczenia albo rozszerzenia zakresu może być dokonana poprzez przesłanie przez Powierzającego do Procesora nowej zmienionej wersji Załącznika nr 1 w formie elektronicznej (na adres e-mail wskazany w Załączniku nr 4). W przypadku braku reakcji Procesora w ciągu 3 dni roboczych (dalej również: „Dni Robocze") od daty wysłania wiadomości przez Powierzającego przyjmuje się, że Procesor zaakceptował zmianę zakresu powierzenia.
3. Dane osobowe przetwarzane są w celu realizacji Umowy Głównej. Procesor zobowiązuje się do przetwarzania powierzonych mu danych osobowych wyłącznie w zakresie i celu niezbędnym do realizacji obowiązków wynikających z Umowy Głównej.
4. W stosunku do danych osobowych podejmowane mogą być następujące kategorie czynności przetwarzania, np.: przeglądanie, przechowywanie.
5. Z tytułu przetwarzania danych osobowych Procesorowi nie przysługuje prawo do odrębnego wynagrodzenia poza wskazanym w Umowie Głównej (w tym również na wypadek zmiany zakresu przetwarzania).

§ 2
Obowiązki i Odpowiedzialność Stron

1. Procesor oświadcza, że zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
2. W przypadku, gdy Procesor stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO, jest to wystarczające do wykazania zapewnienia gwarancji, o których mowa w ustępie poprzedzającym w zakresie objętym zatwierdzonym kodeksem postępowania lub zatwierdzonym mechanizmem certyfikacji.
3. Procesor zobowiązany jest:
1) przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Powierzającego, co dotyczy także przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, chyba że obowiązek taki wynika z powszechnie obowiązujących przepisów prawa. Powierzający może przekazywać Procesorowi dokładniejsze instrukcje poprzez zgłoszenie w serwisie Procesora dedykowanym do obsługi zgłoszeń.
2) niezwłocznie informować Powierzającego o obowiązku prawnym udostępnienia danych osobowych, o którym mowa w pkt. 1) powyżej, chyba że powszechnie obowiązujące przepisy zabraniają udzielania takiej informacji z uwagi na ważny interes publiczny;
3) dopuszczać do przetwarzania danych osobowych wyłącznie osoby odpowiednie, upoważnione do tego;
4) dopuszczać do przetwarzania danych osobowych wyłącznie osoby, które zobowiązały się do zachowania tajemnicy, lub które podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
5) jeżeli dane osobowe powierzone Procesorowi do przetwarzania zawierają dane o stanie zdrowia oraz podlegają tajemnicy zawodowej osób wykonujących zawody medyczne, procesowania ich z zachowaniem najwyższej staranności, w tym zakresie zasad bezpieczeństwa i zabezpieczeń systemów informatycznych oraz innych obowiązków wynikających z przepisów prawa, w szczególności ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz Umowy;
6) podejmować wszelkie środki wymagane, zgodnie z art. 32 RODO, z uwzględnieniem stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający temu ryzyku, w szczególności:
a) pseudonimizację i szyfrowanie danych osobowych,
b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
c) zdolność do szybkiego przywrócenia danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,
7) przestrzegać warunków korzystania z usług podmiotu, któremu podpowierza przetwarzanie danych osobowych, wskazanych w ust. 14 i 15 poniżej,
8) w razie potrzeby i na żądanie Powierzającego pomagać Powierzającemu poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO; w szczególności dotyczy to wspomagania w zakresie udzielania odpowiedzi na wniosek o korzystanie z praw osoby, których dane dotyczą, w tym w zakresie prawa dostępu przysługującego osobie, której dane dotyczą, prawa do sprostowania danych, prawa do usunięcia danych, prawa do ograniczenia przetwarzania,
9) niezwłocznie, nie później jednak niż w terminie 2 dni roboczych na adres wskazany w Załączniku nr 4 informować Powierzającego o tym, iż osoba, której dane dotyczą, skierowała do Procesora korespondencję zawierającą żądanie w zakresie wykonywania praw osoby określonych w rozdziale III RODO, jak również udostępniać treść tej korespondencji,
10) w razie potrzeby i/lub na żądanie Powierzającego pomagać Powierzającemu wywiązywać się z następujących obowiązków:
a) wypełniania obowiązków związanych z wdrożeniem odpowiednich środków technicznych i organizacyjnych dla zapewnienia bezpieczeństwa przetwarzania przez Powierzającego, zgodnie z art. 32 RODO,
b) zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu zgodnie z art. 33 RODO,
c) zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z art. 34 RODO,
d) dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych zgodnie z art. 35 RODO,
e) przeprowadzaniu konsultacji z organem nadzorczym zgodnie art. 36 RODO,
11) udostępniać Powierzającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków w zakresie powierzenia przetwarzania danych, o ile nie stanowią one tajemnicy przedsiębiorcy lub innej tajemnicy prawnie chronionej. Procesor jest zobowiązany udostępnić co najmniej do wglądu wszelkie informacje i dokumenty w terminie 2 Dni Roboczych od przesłania żądania Powierzającego na adres wskazany w Załączniku nr 4.
4. Procesor zobowiązany jest prowadzić rejestr wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu Powierzającego, zawierający następujące informacje:
1) imię i nazwisko lub nazwę oraz dane kontaktowe Procesora oraz Powierzającego, a gdy ma to zastosowanie – przedstawiciela Procesora oraz inspektora ochrony danych,
2) kategorie przetwarzań dokonywanych w imieniu Powierzającego,
3) gdy ma to zastosowanie – informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO dokumentację odpowiednich zabezpieczeń,
4) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
5. Procesor jest zobowiązany do wdrożenia i stosowania procedur służących wykrywaniu naruszeń ochrony danych osobowych oraz wdrażania właściwych środków naprawczych. Procesor jest zobowiązany do udostępnienia procedur, o których mowa w zdaniu poprzedzającym, co najmniej do wglądu, na żądanie Powierzającego przekazane za pośrednictwem e-maila na adres wskazany w Załączniku nr 4. Procesor jest zobowiązany do udzielenia odpowiedzi w terminie 3 Dni Roboczych od przesłania przez Powierzającego żądania.
6. Po stwierdzeniu naruszenia ochrony danych osobowych Procesor bez zbędnej zwłoki, jednak nie później niż 24 godzin od powzięcia wiadomości o naruszeniu, zgłasza ten fakt Powierzającemu, wskazując w zgłoszeniu:
1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie oraz przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
2) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
3) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
4) opis środków zastosowanych lub proponowanych przez Procesora w celu zapobieżenia naruszenia ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.
7. Zgłoszenie naruszenia ochrony danych osobowych następuje na adres mailowy wskazany w Załączniku nr 4.
8. Jeśli wszystkich informacji, o których mowa w ust. 6 powyżej, nie da się udzielić w tym samym czasie, Procesor ma obowiązek ich udzielać Powierzającemu sukcesywnie bez zbędnej zwłoki.
9. Do czasu przekazania Procesorowi instrukcji postępowania w związku z naruszeniem ochrony danych, Procesor podejmuje bez zbędnej zwłoki wszelkie działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.
10. Bez wyraźnej instrukcji Powierzającego Procesor nie jest zobowiązany do informowania o naruszeniu ochrony danych osobowych organu nadzorczego ani osób, których dane dotyczą.
11. Procesor dokumentuje wszelkie naruszenia ochrony powierzonych mu przez Powierzającego danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze, jak również udostępnia tę dokumentację Powierzającemu na jego żądanie.
12. Procesor ponosi odpowiedzialność za działania swoich pracowników i innych osób, przy pomocy których przetwarza powierzone dane osobowe, jak za własne działanie i zaniechanie.
13. Procesor jest uprawniony do dokonania dalszego powierzenia (podpowierzenia) przetwarzania danych osobowych innemu podmiotowi (dalej również: „Podprocesor") wyłącznie na podstawie uprzedniej ogólnej zgody Powierzającego, która stanowi Załącznik nr 2 do Umowy. Lista podmiotów z których korzysta Procesor stanowi Załącznik nr 3 do Umowy. Powyższe nie wyklucza prawa Procesora do upoważnienia innych podmiotów do przetwarzania danych osobowych powierzonych w ramach Umowy, jednak upoważnienie to musi odbyć się zgodnie z zasadami przewidzianymi w art. 28 ust. 2 RODO. W szczególności Procesor informuje Powierzającego o zamiarze wyboru nowego Podprocesora spoza listy wskazanej w Załączniku nr 3 bez zbędnej zwłoki, nie później jednak niż w terminie 5 dni roboczych od planowanego dnia zawarcia umowy dalszego powierzenia przetwarzania z nowym

Podprocesorem. W sytuacji w której Powierzający wyrazi sprzeciw wobec korzystania przez Procesora z Podprocesora, Procesor nie jest uprawniony do zawarcia umowy z Podprocesorem, którego dotyczy sprzeciw.
14. Jeśli do wykonania, w imieniu Powierzającego, konkretnych czynności przetwarzania Procesor dokona dalszego powierzenia (podpowierzenia) przetwarzania danych osobowych Podprocesorowi, to Procesor zapewnia, iż Podprocesor wypełnia te same obowiązki ochrony danych osobowych, jakie zostały nałożone na Procesora w Umowie, w szczególności obowiązek zapewnienia wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie przez niego danych osobowych było zgodne z wymogami RODO. Procesor ponosi pełną odpowiedzialność za wypełnienie tych obowiązków ochrony danych osobowych przez Podprocesora.
15. W przypadku, gdy Procesor dokonał dalszego powierzenia danych osobowych, Procesor zapewnia, iż Podprocesor wypełniać będzie, bezpośrednio w stosunku do Powierzającego, obowiązki wymienione w ust. 6 oraz ust. 8-9 i ust. 11 powyżej.
16. Procesor zapewni również w umowie z Podprocesorem możliwość realizacji przez Powierzającego kontroli względem dalszego podmiotu przetwarzającego (w tym możliwość przeprowadzania audytów, o których mowa w § 3 Umowy). Procesor jest zobowiązany poinformować Podprocesora, że informacje, w tym dane osobowe, na jego temat mogą być udostępnione Powierzającemu w celu wykonania przez niego uprawnień, o których mowa w zdaniu poprzedzającym.
17. Procesor odpowiada za szkody spowodowane przetwarzaniem danych osobowych w sposób naruszający przepisy RODO, jeśli nie dopełnił obowiązków nałożonych na niego przez RODO lub gdy działał poza zgodnymi z prawem instrukcjami Powierzającego lub wbrew tym instrukcjom.
18. Procesor ma obowiązek współdziałać z Powierzającym na jego żądanie w zakresie ustalenia przyczyn szkody wyrządzonej osobie, której dane dotyczą, jak również zapewnia, że obowiązek ten będzie wypełniać bezpośrednio Podprocesor w stosunku do Powierzającego.
19. W przypadku, gdy za szkodę spowodowaną przetwarzaniem odpowiadają zarówno Powierzający, jak i Procesor, ponoszą oni odpowiedzialność solidarną za całą szkodę. Powierzający lub Procesor nie ponosi odpowiedzialności, o którym mowa w zdaniu poprzednim, jeżeli w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.
20. W przypadku, gdy Powierzający zapłacił odszkodowanie za całą wyrządzoną szkodę spowodowaną przetwarzaniem, ma prawo żądania od Procesora zwrotu części odszkodowania odpowiadającej części szkody, za którą ponosi on odpowiedzialność.
21. Niezwłocznie, jednak nie później niż w ciągu 2 Dni Roboczych Procesor zobowiązany jest informować (o ile nie doprowadzi to do naruszenia przepisów obowiązującego prawa) Powierzającego o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych przez Procesora, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych, skierowanej do Procesora, o wszelkich kontrolach i inspekcjach dotyczących przetwarzania danych osobowych przez Procesora, w szczególności prowadzonych przez organ nadzoru, a także o wszelkich skargach osób, których dane dotyczą związanych z przetwarzaniem ich danych osobowych.
22. Każda ze Stron odpowiada za szkody wyrządzone drugiej Stronie oraz osobom trzecim w związku z powierzeniem przetwarzania danych, zgodnie z przepisami Kodeksu cywilnego, z zastrzeżeniem postanowień RODO wskazanych powyżej.

§3

Prawo kontroli

1. Powierzający posiada prawo kontroli właściwego przetwarzania przez Procesora powierzonych mu danych osobowych. Procesor na każdy pisemny wniosek Powierzającego zobowiązany jest do udzielenia pisemnej informacji dotyczącej przetwarzania powierzonych mu danych osobowych, w terminie 5 Dni Roboczych od dnia otrzymania wniosku Powierzającego.
2. Procesor umożliwia Powierzającemu lub upoważnionemu przez Powierzającego audytorowi przeprowadzenie audytów, w tym inspekcji, i zobowiązuję się współpracować z Powierzającym w zakresie dotyczącym wyłącznie realizacji Umowy. Powierzający zobowiązuje się, że jako upoważniony audytor nie zostanie wyznaczony podmiot prowadzący pośrednio lub bezpośrednio działalność konkurencyjną w stosunku do działalności prowadzonej przez Procesora. Ewentualne czynności kontrolne będą prowadzone na koszt i ryzyko Powierzającego.
3. Termin przeprowadzenia kontroli zostanie ustalony z Procesorem, jednak kontrola nie może odbyć się później niż 5 Dni Roboczych od przekazania Procesorowi żądania na adres mailowy wskazany w Załączniku nr 4.
4. Procesor niezwłocznie informuje Powierzającego, jeśli wydane Procesorowi polecenie, w oparciu o § 2 ust. 3 pkt 10 Umowy lub w oparciu o ust. 1 powyżej, stanowi naruszenie RODO lub innych powszechnie obowiązujących przepisów.
5. Po przeprowadzonym audycie przedstawiciel Powierzającego lub upoważniony przez Powierzającego przedstawiciel audytora sporządza protokół pokontrolny, który podpisują przedstawiciele obu Stron. Procesor zobowiązuje się w terminie uzgodnionym z Powierzającym, dostosować do zaleceń pokontrolnych zawartych w protokole, mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
6. Powierzający ma także prawo żądać od Procesora składania pisemnych wyjaśnień dotyczących realizacji Umowy. Procesor zobowiązuje się odpowiedzieć niezwłocznie, jednak nie później niż w terminie 3 Dni Roboczych, na każde pytanie Powierzającego dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.
7. Procesor jest zobowiązany zapewnić w umowie z dalszym podmiotem przetwarzającym możliwość przeprowadzania przez Powierzającego (lub podmiot zewnętrzny, któremu Powierzający zleci wykonanie audytu) audytu zgodności przetwarzania danych osobowych przez dalszy podmiot przetwarzający z Umową na zasadach określonych w § 3 ust. 1 – 3.
8. Koszty związane z przeprowadzeniem audytu ponosi podmiot, który zlecił przeprowadzenie audytu, bez prawa do żądania zwrotu takich kosztów ani zapłaty dodatkowego wynagrodzenia.
9. W przypadku, gdy Procesor audytowany jest za zgodność z przepisami RODO przez niezależny podmiot trzeci z własnej inicjatywy, Procesor zobowiązuje się udostępnić Powierzającemu na jego żądanie wyniki tego audytu bez zbędnej zwłoki, nie później niż w terminie 3 dni roboczych. Wyniki audytu obejmują informacje o stwierdzonym stopniu zgodności z RODO i podstawowe wnioski z audytu. Wyniki audytu mogą zawierać szczegółowe informacje, w tym protokół, w zakresie, w jakim nie ujawniają tajemnicy przedsiębiorcy lub innej tajemnicy prawnie chronionej.

§ 4

Wsparcie Powierzającego w wykonywaniu praw określonych w rozdziale III RODO

1. Zgodnie z art. 28 ust. 3 pkt. e) RODO biorąc pod uwagę charakter przetwarzania, Procesor w miarę możliwości pomaga Powierzającemu poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO.
2. Procesor jest zobowiązany do wsparcia Powierzającego w zakresie realizacji następujących praw podmiotów danych osobowych:
a) obowiązku informacyjnego przewidzianego w art. 13 i art. 14 RODO;
b) prawa dostępu do danych;
c) prawa do sprostowania danych;
d) prawa do usunięcia danych;
e) prawa do ograniczenia przetwarzania;
f) obowiązku poinformowania o sprostowaniu lub usunięciu danych lub o ograniczeniu przetwarzania;
g) prawa do przenoszenia danych;
h) prawa do sprzeciwu;
i) kwestii związanych z prawem do niepodlegania zautomatyzowanemu przetwarzaniu danych, w tym profilowaniu.
3. Żądanie Powierzającego w zakresie uzyskania wsparcia w związku z realizacją praw wymienionych w pkt. 2 zostanie niezwłocznie przekazane Procesorowi na adres mailowy wskazany w Załączniku nr 4.
4. Procesor w ciągu 2 Dni Roboczych od otrzymania żądania potwierdzi jego otrzymanie Powierzającemu.
5. Procesor w terminie 5 Dni Roboczych od terminu wskazanego w ust. 4 poinformuje Powierzającego o wykonaniu przekazanego żądania.
6. Jeżeli Procesor nie jest w stanie zrealizować żądania przekazanego mu przez Powierzającego jest on zobowiązany do przygotowania i przekazania Powierzającemu wyjaśnienia opisującego przyczyny dla których zrealizowanie żądania Powierzającego było niemożliwe.

§ 5

Transfer danych osobowych do państw trzecich

1. Procesor nie może przekazywać (transferować) danych osobowych do państwa trzeciego, które znajduje się poza Europejskim Obszarem Gospodarczym (dalej również: „EOG”), chyba że Powierzający udzieli mu uprzedniej, pisemnej pod rygorem nieważności, zgody zezwalającej na taki transfer.
2. Jeśli Powierzający udzieli Procesorowi uprzedniej zgody na przekazanie danych osobowych do państwa trzeciego, Procesor może dokonać transferu tych danych osobowych tylko wtedy, gdy:
a) państwo docelowe zapewnia adekwatny poziom ochrony danych osobowych do tego, który obowiązuje w Unii Europejskiej lub
b) Powierzający i Procesor lub Podprocesor zawarli umowę w oparciu o standardowe klauzule umowne lub wdrożyli inny mechanizm, który zgodnie z przepisami prawa legalizuje transfer danych do państwa trzeciego.

§ 6

Adresy stron i dane osób

1. Wszelka korespondencja w sprawach związanych z Umową będzie kierowana na adresy Stron wskazane w Załączniku nr 4.
2. Procesora w kontaktach z Powierzającym oraz Powierzający w kontaktach z Procesorem w zakresie ustaleń Umowy reprezentować będą osoby wskazane w Załączniku nr 4.
3. Zmiana adresów i danych tych osób nie stanowi zmiany Umowy. O każdej zmianie danych zawartych w Załączniku nr 4, Strony powiadomią się na piśmie, za potwierdzeniem odbioru lub drogą elektroniczną.

§ 7

Czas trwania Umowy

1. Powierzenie trwa przez czas obowiązywania Umowy Głównej. W celu uniknięcia wątpliwości, rozwiązanie Umowy Głównej skutkuje rozwiązaniem Umowy.
2. Po zakończeniu świadczenia usług związanych z przetwarzaniem Procesor ma obowiązek usunąć lub zwrócić Powierzającemu – zależnie od decyzji Powierzającego – wszelkie dane osobowe, które zostały mu powierzone, jak również usunąć wszelkie ich istniejące kopie, chyba że powszechnie obowiązujące przepisy nakazują przechowywanie tych danych osobowych.
3. Procesor przesyła Powierzającemu pisemne potwierdzenie zniszczenia danych osobowych. Potwierdzenie powinno zostać przesłane na adres e-mail wskazany w Załączniku nr 4.
4. Powierzający jest uprawniony do rozwiązania Umowy bez wypowiedzenia, jeżeli Procesor nie wypełnia obowiązków wskazanych w § 2 Umowy, lub uniemożliwia Powierzającemu skorzystania z prawa kontroli wskazanego w § 3 Umowy.
5. W przypadku podpowierzenia przetwarzania danych osobowych Procesor zobowiązuje się do zawarcia w umowach z Podprocesorami postanowień, zgodnie z którymi umowy podpowierzenia danych będą ulegały automatycznemu rozwiązaniu w razie zakończenia obowiązywania niniejszej Umowy.

§ 8

Postanowienia końcowe

1. Niniejsza Umowa podlega prawu polskiemu.
2. W sprawach, które nie zostały uregulowane Umową, znajdują zastosowanie odpowiednie przepisy Kodeksu cywilnego, RODO oraz innych obowiązujących przepisów z zakresu ochrony danych osobowych, a także przepisy regulujące prawa pacjenta, zasady wykonywania zawodów medycznych oraz prowadzenia działalności leczniczej.
3. Zmiany Umowy są możliwe wyłącznie w formie pisemnej pod rygorem nieważności, z zastrzeżeniem sytuacji, w których Umowa wprost przewiduje inną formę dokonywania zmian.
4. Procesor nie może przenieść praw lub obowiązków wynikających z niniejszej Umowy bez pisemnej zgody Powierzającego.

5. O ile Umowa główna nie stanowi inaczej, wszelkie spory w związku z niniejszą Umową zostaną poddane pod rozstrzygnięcie sądu powszechnego miejscowo właściwego ze względu na siedzibę Powierzającego.
[6. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej Strony.] – nie dotyczy umów zawieranych w formie elektronicznej

W imieniu powierzającego
…….

W imieniu procesora
……..

ZAŁĄCZNIK NR 1

ZAKRES PRZETWARZANIA

Kategoria osób, których dane dotyczą	Rodzaj danych osobowych

ZAŁĄCZNIK NR 2
PISEMNA ZGODA POWIERZAJĄCEGO NA KORZYSTANIE PRZEZ PROCESORA Z USŁUG PODPROCESORÓW

Działając w imieniu Powierzającego, zgodnie z § 2 ust. 13 Umowy, niniejszym wyrażam zgodę na korzystanie przez Procesora z Podprocesorów w ramach świadczenia usług na podstawie niniejszej Umowy.

Oświadczam, iż Procesor przedstawił mi listę Podprocesów z których usług korzysta. Lista stanowi załącznik nr 3 do Umowy.

W imieniu Powierzającego

……

ZAŁĄCZNIK NR 3

LISTA PODPROCESORÓW Z USŁUG KTÓRYCH KORZYSTA PROCESOR

……

ZAŁĄCZNIK NR 4

DANE KONTAKTOWE STRON

Dane przedstawicieli Stron:

Wszelka korespondencja w sprawach związanych z Umową będzie kierowana do Powierzającego na następujące dane kontaktowe: adres Wojewódzki Szpital Specjalistyczny w Legnicy tel. 76/ 72-11-300, email sekretariat@szpital.legnica.pl Powierzającego w kontaktach z Procesorem w zakresie ustaleń Umową reprezentować będą następujące osoby: Krzysztof Maciejak, tel. 76/72-11-707, email: iod@szpital.legnica.pl

Wszelka korespondencja w sprawach związanych z Umową będzie kierowana do Procesora na następujące dane kontaktowe: adres ……, tel. …….., email ……
Procesora w kontaktach z Powierzającym w zakresie ustaleń Umową reprezentować będą następujące osoby:
……..
adres ……, tel. ……, email ……

Procesor **Powierzający**

Rozdział VIII. Informacje o środkach komunikacji elektronicznej, przy użyciu których Zamawiający będzie komunikował się z Wykonawcami oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej

1.W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcą odbywa się w godzinach pracy od 7.25 do 15.00, z wyłączeniem dni ustawowo wolnych od pracy.
2. Komunikacja pomiędzy Zamawiającym a wykonawcami w szczególności składanie oświadczeń, zawiadomień, zapytań oraz przekazywanie informacji odbywa się przy użyciu środków komunikacji elektronicznej za pośrednictwem:

https://platformazakupowa.pl/pn/szpital_legnica i formularza ***Wyślij wiadomość*** dostępnego na stronie internetowej prowadzonego postępowania.
3. W sytuacjach awaryjnych np. w przypadku braku działania https://platformazakupowa.pl/pn/szpital_legnica Zamawiający może również komunikować się z wykonawcami za pomocą poczty elektronicznej na adres dorota.kunigielis@szpital.legnica.pl
4. Postępowanie jest prowadzone w języku polskim.
5. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem *https://platformazakupowa.pl/pn/szpital_legnica* jako załączniki. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie.
6. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.
7. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, nie później jednak niż na 2 dni przed upływem terminu składania ofert, pod warunkiem że wniosek o wyjaśnienie treści SWZ wpłynie do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
8. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 7, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych Wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert.
9. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ, o którym mowa w ust. 7.
10. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ust. 7, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
11. Treść zapytań wraz z wyjaśnieniami Zamawiający udostępnia na stronie internetowej prowadzonego postępowania, przekazuje Wykonawcom, którym przekazał SWZ, bez ujawniania źródła zapytania.

Rozdział IX. Wskazanie osób uprawnionych do komunikowani a się z Wykonawcami

Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami:
1) Dorota Kunigielis – Sekcja Zamówień Publicznych Zamawiającego,
2) Andrzej Biesaga – Dział Infomatyczny

Rozdział X. Termin związania ofertą

1.Wykonawca jest związany ofertą od dnia upływu terminu składania ofert **do 20-10-2023 r.**
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, Zamawiający przed upływem terminu związania oferta zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
4. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający wezwie Wykonawcę, którego oferta otrzymała najwyższą ocenę do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty.
5. W przypadku braku zgody, o której mowa w ust.4, oferta podlega odrzuceniu, a Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania.

Rozdział XI. Opis sposobu przygotowania oferty

1. Ofertę należy przygotować w języku polskim. Do przygotowania i złożenia oferty:
1) konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy kwalifikowanego podpisu elektronicznego, podpisu zaufanego lub podpisu osobistego,
2) zaleca się wykorzystanie Formularza ofertowego (stanowiącego Załącznik 2 do SWZ). W przypadku, gdy Wykonawca nie korzysta z przygotowanych przez Zamawiającego wzorów, w treści oferty należy zamieścić wszystkie informacje tam wymagane.
2. Do oferty należy dołączyć:
1) Oświadczenie o niepodleganiu wykluczeniu z udziału w postępowaniu (wzór oświadczenia w Załączniku 1 do SWZ) – w przypadku Wykonawców składających wspólnie ofertę, oświadczenie składa każdy z Wykonawców z osobna
2) Pełnomocnictwo upoważniające do złożenia oferty, o ile ofertę składa pełnomocnik;
3) Pełnomocnictwo dla pełnomocnika do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia;
4) Dokument potwierdzający wniesienie wadium (o ile nie jest wnoszone w pieniądzu na konto Zamawiającego).
3. Składanie ofert przez Wykonawców winno być przeprowadzone zgodnie z Instrukcją dla wykonawców dostępną na stronie wwww.platformazakupowa.pl w zakładce Instrukcje.
4. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj. Dz.U. 2020 poz. 1913, ze zm.), które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny

zostać załączone w osobnym miejscu w kroku 1 składania oferty przeznaczonym na zamieszczanie tajemnicy przedsiębiorstwa. Zaleca się, aby każdy dokument zawierający tajemnicę przedsiębiorstwa został zamieszczony w odrębnym pliku.
Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 uPzp.
5. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (t.j. w formie elektronicznej). Dopuszcza się także złożenie elektronicznej kopii(skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez upełnomocnionego.

Rozdział XII. Sposób oraz termin składania ofert

1.Wykonawca składa ofertę za pośrednictwem **Formularza do złożenia oferty** dostępnego na: **https://platformazakupowa.pl/pn/szpital_legnica**. Składanie ofert przez Wykonawców winno być przeprowadzone zgodnie z Instrukcją dostępną na www.platformazakupowa.pl w zakładce Instrukcje.
2. Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie do dnia **03-10-2023 r. o godzinie 11.00**
3. Wykonawca może złożyć jedną ofertę. Złożenie więcej niż jednej oferty spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.
4. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
5. Wykonawca przed upływem terminu do składania ofert może wycofać ofertę. Sposób wycofania oferty został opisany w Instrukcji na stronie www.platformazakupowa.pl w zakładce Instrukcje.
6. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.

Rozdział XIII. Termin otwarcia ofert

1. Otwarcie ofert nastąpi w dniu **03-10-2023 r. o godzinie 11.30.**
2. Zamawiający, najpóźniej przed otwarciem ofert, udostępniani na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
3. Zamawiający, niezwłocznie po otwarciu ofert udostępni na stronie internetowej prowadzonego postępowania informacje o:
1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte;
2) cenach zawartych w ofertach.
4. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwościowi otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
5. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

Rozdział XIV. Podstawy wykluczenia

1. Z postępowania o udzielenie zamówienia wyklucza się, z zastrzeżeniem art. 110 ust. 2 uPzp, Wykonawcę:
1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
c) o którym mowa w art. 228–230a, art. 250a Kodeksu karnego, w art. 46–48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust. 1–4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2021 r. poz. 523, 1292, 1559 i 2054),
d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2021 poz. 1745) ,

g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe,
h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej – lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
5) jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe, chyba że wykażą, że przygotowali te oferty niezależnie od siebie;
6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 uPzp, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z Wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.
2. Okres wykluczenia Wykonawcy z postępowania o udzielenie zamówienia publicznego określony został w Art. 111 uPzp.
3. Niezależnie od powyższego Zamawiający wykluczy z postępowania Wykonawcę, który podlega wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego*, zwanej w niniejszym ust. „ustawą", to jest:
1) Wykonawcę wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanym na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
2)Wykonawcę, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
3) Wykonawcę, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. *o rachunkowości* (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

Rozdział XV. Sposób obliczenia ceny

1. Wykonawca określa cenę za przedmiot zamówienia poprzez wskazanie w ofercie ceny brutto (określonej w Załączniku 2) .
2. Cena musi być wyrażona w złotych polskich. Zaleca się, aby poszczególne ceny jednostkowe netto były określone do 2 miejsc po przecinku, ale dopuszczalne jest zastosowanie do 4 miejsc po przecinku w przypadku gdy wymaga tego prawidłowe złożenie oferty. Całkowita wartość zamówienia (netto i brutto) w powinna być wyrażona w złotych polskich z dokładnością do dwóch miejsc po przecinku - związku z tym, Wykonawca powinien zaokrąglić wykazane kwoty tj. jeżeli obliczana cena ma więcej miejsc po przecinku należy ją zaokrąglić w ten sposób, że cyfry od 1 do 4 należy zaokrąglić w dół, natomiast cyfry od 5 do 9 należy zaokrąglić w górę.
3. Cena oferty musi zawierać wszelkie koszty niezbędne do zrealizowania zamówienia wynikające wprost z SWZ, jak również koszty w nich nie ujęte np. dojazd do Zamawiającego tam i z powrotem, itp., a bez których nie można wykonać przedmiotu zamówienia (również ewentualne opusty oferowane przez Wykonawcę), w szczególności w cenie należy uwzględnić wszelkie dodatkowe koszty, jakie poniesie Wykonawca z tytułu należytej realizacji przedmiotu umowy. (w tym również ew. koszty związane ze wzrostem kursów walut itp.) .
4. Jeżeli Wykonawca złoży ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. W takim przypadku Wykonawca zobowiązany jest do:
1) poinformowania Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;
2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;

3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku;
4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.
5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich.

Rozdział XVI. Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Zamawiający dokona oceny ofert, które nie zostały odrzucone, na podstawie następujących kryteriów oceny ofert:
1) Cena (C) - 60 %
2) Okres gwarancji i rękojmi dla zaoferowanej biblioteki taśmowej* (GRB) – 20 %
*- ocenie podlegać będzie zaoferowany okres gwarancji i rękojmi dla biblioteki taśmowej, przy czym nie może być on krótszy niż 60 miesięcy i dłuższy niż 84 miesiące
3) Okres gwarancji i rękojmi dla zaoferowanego serwera** (GRS) – 20 %
**- ocenie podlegać będzie zaoferowany okres gwarancji i rękojmi dla serwera, przy czym nie może być on krótszy niż 60 miesięcy i dłuższy niż 84 miesiące

Punkty w kryterium „Cena" zostaną obliczone według wzoru:

$$C = \frac{\text{Cena oferty najtańszej – wartość brutto}}{\text{Cena oferty badanej – wartość brutto}} \text{ razy } 60 = \text{liczba punktów}$$

Punkty w kryterium „Okres gwarancji i rękojmi dla zaoferowanej biblioteki taśmowej" zostaną obliczone wg wzoru:

$$GRB = \frac{\text{Okres gwarancji i rękojmi w badanej ofercie}}{\text{Najdłuższy okres gwarancji i rękojmi z spośród złożonych ofert}} \text{ razy } 20 = \text{liczba punktów}$$

Punkty w kryterium „Okres gwarancji i rękojmi dla zaoferowanego serwera" zostaną obliczone wg wzoru:

$$GRS = \frac{\text{Okres gwarancji i rękojmi w badanej ofercie}}{\text{Najdłuższy okres gwarancji i rękojmi z spośród złożonych ofert}} \text{ razy } 20 = \text{liczba punktów}$$

Ad .2) i Ad. 3) **„Okres gwarancji i rękojmi"** w przypadku:
a) braku podania przez Wykonawcę wartości dotyczącej oferowanego okresu, przyjmie się najniższą wartość przewidzianą w SWZ, tzn. 60 miesięczny okres. Określona w ten sposób wartość będzie wiążąca dla Wykonawcy i zostanie wprowadzona do umowy,
b) zaoferowania okresu dłuższego niż 84 miesiące, Zamawiający przyzna punkty, jak dla wartości 84 miesięcy, natomiast do umowy zostanie wprowadzona wartość zaoferowana przez Wykonawcę.
c) zaoferowania terminu krótszego niż 60 miesięcy – będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt 5) uPzp – tj. jako treść niezgodna z warunkami zamówienia.
2. Za najkorzystniejszą uznana zostanie oferta z największą liczbą punktów, tj. przedstawiająca najkorzystniejszy bilans kryteriów oceny ofert, o których mowa powyżej.
3. W przypadku, gdy Zamawiający podejmie decyzję o nieprzeprowadzaniu negocjacji - za najkorzystniejszą zostanie uznana oferta dodatkowa z największą liczbą punktów, tj. przedstawiająca najkorzystniejszy bilans ocenianych kryteriów, o których mowa powyżej. Punkty będą przyznawane do dwóch miejsc po przecinku.

Rozdział XVII. Informacje związane z negocjacjami i ofertami dodatkowymi

1. W przypadku, podjęcia przez Zamawiającego decyzji o przeprowadzeniu negocjacji:
1) wszyscy Wykonawcy, którzy w odpowiedzi na ogłoszenie o zamówieniu złożyli oferty, zostaną równocześnie poinformowani, o Wykonawcach:
a) których oferty nie zostały odrzucone, oraz punktacji przyznanej ofertom w kryterium oceny ofert (zgodnie z kryterium określonym i opisanymi w Rozdziale XVI SWZ),
b) których oferty zostały odrzucone,
- ze wskazaniem uzasadnienia faktycznego i prawnego;
2) w zaproszeniu do negocjacji Zamawiający wskaże miejsce, termin i sposób prowadzenia negocjacji oraz kryteria oceny ofert, w ramach których będą prowadzone negocjacje w celu ulepszenia treści ofert;
3)poinformuje równocześnie wszystkich Wykonawców o zakończeniu negocjacji oraz zaprosi ich do składania ofert dodatkowych, wskazując co najmniej:
a) nazwę oraz adres Zamawiającego, numer telefonu, adres poczty elektronicznej oraz strony internetowej prowadzonego postępowania;
b) sposób i termin składania ofert dodatkowych oraz język lub języki, w jakich muszą one być sporządzone, oraz termin otwarcia tych ofert.

2. Podczas negocjacji ofert Zamawiający zapewnia równe traktowanie wszystkich Wykonawców. Zamawiający nie udziela informacji w sposób, który mógłby zapewnić niektórym wykonawcom przewagę nad innymi Wykonawcami.
3. Zamawiający wyznaczy termin na złożenie ofert dodatkowych z uwzględnieniem czasu potrzebnego na przygotowanie tych ofert, z tym że termin ten nie będzie być krótszy niż 5 dni od dnia przekazania zaproszenia do składania ofert dodatkowych.
4. Wykonawca może złożyć ofertę dodatkową, która zawiera nowe propozycje w zakresie treści oferty podlegających ocenie w ramach kryteriów oceny ofert wskazanych przez zamawiającego w zaproszeniu do negocjacji.
5. Oferta dodatkowa nie może być mniej korzystna w żadnym z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu. Oferta przestaje wiązać Wykonawcę w zakresie, w jakim złoży on ofertę dodatkową zawierającą korzystniejsze propozycje w ramach każdego z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji. Oferta dodatkowa, która b mniej korzystna w którymkolwiek z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu, podlega odrzuceniu.
6. Za najkorzystniejszą zostanie uznana oferta z największą liczbą punktów, tj. przedstawiające najkorzystniejszy bilans ocenianych kryteriów. Punkty będą przyznawane do dwóch miejsc po przecinku.

Rozdział XVIII. Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577 uPzp, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertę.
3. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy wskazanych w Rozdziale VII SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.
4. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty jako najkorzystniejszej) przedstawią Zamawiającemu umowę regulującą współpracę tych Wykonawców.
5. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.
6. Dopuszcza się zawarcie umów w formie elektronicznej.

Rozdział XIX. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów uPzp.
2. Odwołanie przysługuje na:
1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie uPzp.
3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.
4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.
5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX uPzp „Środki ochrony prawnej"

Rozdział XX. Opis Części zamówienia

Zamawiający nie dopuszcza składania ofert częściowych. Zamawiający zawarł w dniu 31-08-2023 r. umowę Narodowym Funduszem Zdrowia „Umowa o dodatkowe finansowanie", która zgodnie z „Zarządzeniem" - Prezesa Narodowego Fundusz Zdrowia winna zostać rozliczona w terminie do dnia 24 października 2024 r. Brak podziału zamówienia na części podyktowany jest terminowym rozliczeniem środków finansowych na cyberbezpieczeństwo.

Rozdział XXI. Liczba Części zamówienia, na którą Wykonawca może złożyć ofertę

Nie dotyczy niniejszego postępowania.

Rozdział XXII. Informacje o liczbie Wykonawców, których Zamawiający zaprosi do negocjacji

Zamawiający nie będzie ograniczał liczby Wykonawców zaproszonych do negocjacji.

Rozdział XXIII. Informacje o przedmiotowych środkach dowodowych

Zamawiający nie wymaga złożenia przedmiotowych środków dowodowych.

Rozdział XXIV. Załączniki do SWZ

1) Wzór Oświadczenia Wykonawcy, o którym mowa w art. 125 ust.1 oraz w zakresie podlegania wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* – Załącznik 1,
2) Wzór formularza ofertowego – Załącznik 2,

Rozdział XXV. Klauzula informacyjna dotycząca przetwarzania danych osobowych

1. Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady(UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)(Dz.Urz.UEL119 z 04.05.2016, str.1), dalej„RODO”, informuję, że:
•administratorem Pani/Pana danych osobowych jest Wojewódzki Szpital Specjalistyczny w Legnicy
•w sprawach związanych z Pani/Pana danymi proszę kontaktować się z Inspektorem Ochrony Danych, kontakt pisemny za pomocą poczty tradycyjnej na adres: Wojewódzki Szpital Specjalistyczny w Legnicy, 59-220 Legnica, ul. Iwaszkiewicza 5;
pocztą elektroniczną na adres e-mail: iod@szpital.legnica.pl
•Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust.1lit. C RODO w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego oraz zawarcia umowy, a podstawą prawną ich przetwarzania jest obowiązek prawny stosowania sformalizowanych procedur udzielania zamówień publicznych spoczywający na Zamawiającym;
•odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art.18 oraz art. 74 uPzp;
•Pani/Pana dane osobowe będą przechowywane, zgodnie z art.78 ust.1 uPzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
•obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach uPzp, związanym z udziałem w po-stępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z uPzp;
•w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
•Posiada Pan/Pani:
−na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
−na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych, przy czym skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z uPzp oraz nie może naruszać integralności protokołu oraz jego załączników.
−na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art.18 ust.2 RODO, przy czym prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego, a także nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia.
− prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
•nie przysługuje Pani/Panu:
− w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
− prawo do przenoszenia danych osobowych, o którym mowa w art.20 RODO;
− na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust.1 lit. c RODO.
2. Jednocześnie Zamawiający przypomina o ciążącym na Pani/Panu obowiązku informacyjnym wynikającym z art.14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od Wykonawcy biorącego udział w postępowaniu, chyba, że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art.14 ust.5 RODO.

Rozdział XXVI. Szczegółowy opis przedmiotu zamówienia

1) Biblioteka taśmowa 1 sztuka wraz z 40 taśmami

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do zamontowania w szafie rack, maksymalnie 3U, wbudowany czytnik kodów kreskowych, redundantne zasilanie wraz z kablami zasilającymi.
Napęd	Jeden napęd LTO9 FC-FH. Możliwością rozbudowy do min. 20 napędów LTO.

Interfejs	FC wraz z dwoma kablami pozwalającymi na podłączenie do serwera dostarczonego wraz z biblioteką taśmową.
Liczba slotów	40 w tym minimum pięć slotów we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów W komplecie minimum: • 40 taśm LTO9 • 1 taśma czyszczące LTO9 • Etykiety do taśm LT09 o numerach 1-200
Dodatkowe	• interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD • wyjmowane magazynki kieszeni na taśmy w celu łatwego zarządzania większą ilością taśm • wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja) • Obsługa SNMP, TLS1.2 oraz IP6 • Wsparcie dla technologii szyfrowania backupowanych danych.
Warunki gwarancji dla autoloadera	Gwarancja producenta realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. • Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. • W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).

2) Serwer

Parametr	**Charakterystyka (wymagania minimalne)**
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji min. 14 dysków 3,5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 154 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla proponowanego serwera.
RAM	Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do min. 2TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory demand and patrol scrubbing, Failed DIMM isolation, Memory Address Parity Protection
Gniazda PCI	- min. 2 sloty PCIe x16 generacji 3 oraz min. 2 sloty PCIe x16 generacji 4.
Interfejsy sieciowe/FC/SAS	Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (interfejsy nie mogą zajmować gniazda PCI) Wbudowane 2 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP+ (interfejsy nie mogą zajmować gniazda PCI). Porty obsadzone modułami 10Gb/s SFP+ SR. Dodatkowo 2 zewnętrzne interfejsy FC 16Gb/s obsadzone modułami. Serwer wyposażony w 4 światłowody OM3 LC-LC o długości minimum 3 metrów.
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD, NVMe. Zainstalowane dwa dyski min. 480GB SSD SATA Hot-Plug Zainstalowanych dwanaście dysków min. 12TB SAS 7.2 tys. obr/min. 3.5”. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.

Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	min. 2 porty USB 2.0, 1 port micro USB oraz 3 porty USB 3.0, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 750W każdy wraz z kablami zasilającymi o długości min. 2m.
Bezpieczeństwo	Zainstalowany moduł TPM 2.0 Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
System operacyjny	**Windows Server 2022 Standard 16 core lub równoważny***
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla dynamic DNS; - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.
Warunki gwarancji	Gwarancja producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

***- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer 2022 Standard:**

1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
2. Mechanizmy logowania w oparciu o:
   a) login i hasło,
   b) karty z certyfikatami (smartcard),
   c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
3. Praca w roli klienta domeny Microsoft Active Directory.
4. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
5. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
6. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
7. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

8. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
9. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
13. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
20. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
21. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
22. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
23. Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2021/2016.
24. Możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).
25. Dostępne mechanizmy deduplikacji i kompresji na wolumenach.

3) UTM

Informacja podstawowa:

Zamawiający używa aktualnie urządzenia FortiGate 101F, które stanowi jego własność

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa 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.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.
5. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware vCenter (ESXi).

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach umowy powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie

Gwarancja: Urządzenie wraz z oprogramowaniem musi być objęte serwisem gwarancyjnym producenta przez okres 36 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

4) System centralnego logowania, raportowania i korelacji

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.

Parametry wydajnościowe:

1.System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2.Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
    1) Listę najczęściej wykrywanych ataków.
    2) Listę najbardziej aktywnych użytkowników.
    3) Listę najczęściej wykorzystywanych aplikacji.
    4) Listę najczęściej odwiedzanych stron www.
    5) Listę krajów , do których nawiązywane są połączenia.
    6) Listę najczęściej wykorzystywanych polityk Firewall.
    7) Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.
   - Email.
   - IPS.
   - Traffic.
   - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1.System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

2.Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1.System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

2. Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

5) System ochrony poczty elektronicznej

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMWare ESX/ESXi 6.0/6.7/7.0 and later, Citrix XenServer v5.6 SP2/6.0 and later, Microsoft Hyper-V Server 2008 R2/2012/2012 R2/2016/2019, KVM qemu 2.12.1 and later, AWS (Amazon Web Services) Microsoft Azure, Google Cloud Platform

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

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

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

Parametry fizyczne systemu antyspamowego

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

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. 25 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, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
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 dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. 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 (m.in. email bombing).
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 przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:
VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje

System musi być dostarczony w modelu „na własność” tj. Niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
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 36 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

6) System uwierzytelniania, autoryzacji i kontroli dostępu

Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników oraz procesem uwierzytelnienia – w tym celu musi zapewniać wszystkie wymienione poniżej funkcje.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów.

Parametry systemu

Poszczególne elementy wchodzące w skład systemu muszą zapewniać obsługę:

- 4 wirtualnych interfejsów sieciowych.
- Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2010, 2012 R2 oraz 2016; VMware ESXi, ESX wersje:6,7,8; KVM, Xen, Microsoft Azure, AWS, Oracle OCI.

Parametry wydajnościowe i licencyjne

System musi obsługiwać co najmniej:

- Uwierzytelnianie dla 100 użytkowników.
- 100 tokenów dla uwierzytelniania dwuskładnikowego.
- 30 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu).
- Możliwość zdefiniowania co najmniej 10 grup użytkowników,
- 5 lokalnych centrów certyfikacji (CA).
- Możliwość wygenerowania 100 certyfikatów dla użytkowników.

Wymagania ogólne

System musi zapewniać nie mniej niż:

1. Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności.
2. Graficzną reprezentację statusu uwierzytelnionych użytkowników.
3. Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:
   a) Lokalnie.
   b) Zdalnie w oparciu o protokół Syslog.
4. Konfigurację Captive Portalu.

Wymagania funkcjonalne – uwierzytelnianie

Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż:

1. Lokalną, wbudowaną bazę użytkowników.
2. Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo.
3. Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników.
4. Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV.
5. Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:
   a) poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych),
   b) czasu ważności hasła,
6. Konfigurowalną politykę blokowania kont, która będzie uwzględniać:
   a) ilość nieudanych logowań,
   b) czas blokowania konta,
   c) okres nieaktywności, po którym konto jest blokowane.
7. Możliwość odzyskiwania haseł:
   a) z wykorzystaniem adresu email,
   b) z wykorzystaniem pytania pomocniczego.
8. Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować:
   a) wbudowany serwer RADIUS,
   b) integrację z zewnętrznymi serwerami RADIUS – praca jako klient.
9. Obsługę protokołu LDAP, w tym zakresie system musi oferować:
   a) wbudowany serwer LDAP,

   b) możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP).
10. Obsługę protokołu SAML - Identity Provider (IdP) proxy.
11. Realizację funkcji SSO (Single Sign On) w oparciu o:
    a) integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny,
    b) dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows,
    c) kontekst użytkownika przesyłany z serwera RADIUS,
    d) informacje uzyskiwane poprzez protokół Syslog,

Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe

Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie mniej niż:

1. Obsługę dla tokenów sprzętowych (hardware):
   a) wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania.
2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.
3. Dla tokenów na system iOS i Android wymaga się:
   a) aktywacji z centralnego systemu uwierzytelniania (seed provisioning),
   b) możliwości konfiguracji ilości generowanych cyfr (6 lub 8),
   c) generowania kodu (cyfr) co 30 lub 60 sekund,
   d) możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),
   e) ochrony dostępu poprzez konfigurowalny kod PIN,

Możliwość integracji z logowaniem do systemu Windows.

Wymagania funkcjonalne – 802.1x

System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:

1. Obsługa co najmniej poniższych protokołów EAP:
   a) PEAP,
   b) EAP-TTLS,
   c) EAP-TLS,
   d) EAP-GTC.
2. Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication).
3. Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS.

Wymagania funkcjonalne – zarządzanie certyfikatami

System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:

1. Obsługa wbudowanego CA (Certificate Authority).
2. Obsługa CA pośredniczących (Intermediate CA).
3. Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego.
4. Możliwość pobrania wygenerowanych certyfikatów.
5. Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP.
6. Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP.
7. Realizacja CRL (Certificate Revocation List).
8. Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560).
9. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Zarządzanie

1. Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki.
2. System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS.
3. Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć.
4. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Gwarancja oraz wsparcie

Wymaga się aby dostawa obejmowała również serwis producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Zamawiający nie wymaga złożenia przedmiotowych środków dowodowych.

Rozdział XXVII. Informacja o wadium

1. Wykonawca przystępujący do niniejszego postępowania jest obowiązany wnieść wadium na czas związania ofertą w wysokości: **3.400 zł (trzy tysiące czterysta zł)**
2. Wymagane wadium musi być wniesione przed upływem terminu składania ofert.
3. Wadium może być wnoszone w jednej lub kilku następujących formach:
1) pieniądzu;
2) gwarancjach bankowych;
3) gwarancjach ubezpieczeniowych;
4) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2019 r. poz. 310, 836 i 1572).
4. Przy wnoszeniu wadium wykonawca winien powołać się na nazwę niniejszego postępowania: **„DOSTAWA ASORTYMENTU MAJĄCEGO PODNIEŚĆ OCHRONĘ W ZAKRESIE CYBERBEZPIECZEŃSTWA" znak sprawy WSzSL/FZ-69/23**

5. Wadium wnoszone w pieniądzu wpłaca się przelewem na rachunek bankowy Zamawiającego: Wojewódzki Szpital Specjalistyczny w Legnicy, ul. J. Iwaszkiewicza 5, 59-220 Legnica, nr rachunku BGK 36 1130 1033 0018 8002 7220 0012
6. W przypadku wadium wniesionego w formie gwarancji bankowej lub ubezpieczeniowej, udzielona gwarancja musi być gwarancją samoistną, nieodwołalną, bezwarunkową i płatną na pierwsze żądanie, bez konieczności przedkładania jakichkolwiek dodatkowych dokumentów i winna zawierać co najmniej poniższe elementy (lub zapisy równoważne):
a) nazwę dającego zlecenie (Wykonawcy), beneficjenta gwarancji (Zamawiającego), gwaranta (banku lub instytucji ubezpieczeniowej udzielających gwarancji) oraz wskazanie siedzib,
b) określenie wierzytelności, która ma być zabezpieczona gwarancją,
c) kwotę gwarancji,
d) termin ważności gwarancji,
e) zobowiązanie gwaranta do „zapłacenia" kwoty gwarancji na pierwsze pisemne żądanie Zamawiającego zawierające oświadczenie, iż wykonawca, którego ofertę wybrano:
a. odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie,
b. nie wniósł wymaganego zabezpieczenia należytego wykonania umowy;
c. zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie wykonawcy,
oraz, że Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 107 ust. 2 lub art. 128 ust. 1 uPzp, z przyczyn leżących po jego stronie, nie złożył podmiotowych środków dowodowych lub przedmiotowych środków dowodowych potwierdzających okoliczności, o których mowa w art. 57 lub art. 106 ust. 1 uPzp, oświadczenia, o którym mowa w art. 125 ust. 1 uPzp, innych dokumentów lub oświadczeń lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 223 ust. 2 pkt 3 uPzp, co spowodowało brak możliwości wybrania oferty złożonej przez wykonawcę jako najkorzystniejszej.
7. W przypadku wadium wniesionego w formie gwarancji lub poręczenia, o których mowa w ust. 3 pkt 2–4, Wykonawca przekazuje zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej, podpisany przez osoby upoważnione do jego wystawienia.