Piła, dnia luty 2020 r.

EZP.IV-240/15/20/ZO

ZAPYTANIE OFERTOWE

„FORTIGATE 300C" II

1. Zamawiający

Szpital Specjalistyczny w Pile im. Stanisława Staszica
64-920 Piła, ul. Rydygiera 1
tel. (067) 210 62 98
REGON 002161820; NIP 764-20-88-098
http://szpitalpila.pl/

2. Tryb postępowania

Postępowanie prowadzone jest na podstawie § 8 Regulaminu postępowania w sprawach o zamówienia publiczne, który stanowi załącznik do zarządzenia nr 119/2018 Dyrektora Szpitala Specjalistycznego w Pile im. Stanisława Staszica z dnia 19.11.2018 r. – *za pośrednictwem platformy zakupowej:* ***https://platformazakupowa.pl/pn/szpitalpila***

3. Przedmiot zamówienia

3.1. Przedmiotem zamówienia jest **zakup oraz wymiana sprzętu zapory sieciowej tzw. Firewall wraz z oprogramowaniem dla Szpitala Specjalistycznego w Pile im. Stanisława Staszica. Wsparcie techniczne i serwisowe.** Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 2 do zapytania ofertowego.

3.2. Instalacja usługi będzie się odbywać w siedzibie Zmawiającego– na koszt Wykonawcy.

3.3. Wykonawca powinien zapewnić bezpośrednie (na miejscu w szpitalu) wdrożenie aktualizacji i serwisów podanych w zapytaniu.

3.4. Ze względu na krytyczny charakter aktualizacji i serwisów ujętych w zapytaniu (brak ich działania może stanowić zagrożenie dla zabezpieczenia i ochrony danych w szpitalu), czas na przywrócenie ich działania po ewentualnej awarii z uwzględnieniem dojazdu do miejsca usunięcia awarii powinna być nie większa niż 2 godziny.

3.5. Zamawiający nie dopuszcza wykonywania usługi przez podwykonawcę.

3.6. **O udzielenie zamówienia ubiegać się mogą Wykonawcy, którzy potwierdzą spełnienie warunków udziału w postępowaniu – załącznik nr 1 do zapytania ofertowego.**

3.7. Wykonawca zobowiązany jest zrealizować zamówienie na zasadach i warunkach opisanych we wzorze umowy stanowiącym Załącznik nr 3 do SIWZ.

4. Termin wykonania zamówienia oraz warunki płatności

4.1. Wykonawca zrealizuje przedmiot zamówienia określony w pkt 3.1. w terminie **do 20 lutego 2020 r.**

4.2. Czas trwania usługi określonej w pkt 3.4.wynosi - **12 miesięcy od dnia podpisania umowy.**

4.3. Termin płatności wynosi 60 dni od daty doręczenia faktury VAT Zamawiającemu.

5. Wykonawca załączy do oferty następujące dokumenty:

a) aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej,

6. Pozostałe wymagania dotyczące złożenia oferty i dokumentów

6.1. Wykonawca może złożyć tylko jedną ofertę w języku polskim za pośrednictwem **platformy zakupowej, w formie elektronicznej.**

6.2. Zamawiający w toku badania i oceny ofert, w przypadku powstania jakichkolwiek wątpliwości, zastrzega sobie prawo do żądania od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz złożenia dodatkowych dokumentów.

6.3. W imieniu Zamawiającego postępowanie prowadzi Katarzyna Szałowicz tel. 67/ 21 06 298; która to osoba jest upoważniona do kontaktów z Wykonawcami.

6.4. Zamawiający zastrzega sobie prawo do zmiany lub odwołania niniejszego postępowania oraz unieważnienia postępowania na każdym etapie bez podania przyczyny.

00

7. Kryteria oceny:

7.1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Kryteria	*Waga*	*Punktacja*
CENA BRUTTO	100 %	skala 0 – 100 pkt

7.2. Punktacja w kryterium CENA zostanie obliczona z dokładnością do dwóch miejsc po przecinku w następujący sposób:

$$C = \frac{\text{najniższa cena spośród ocenianych ofert}}{\text{cena oferty badanej}} x\ 100\ pkt$$

Gdzie: C – punkty za kryterium CENA przyznane badanej ofercie.

8. Miejsce, termin składania i otwarcia ofert

1. Ofertę należy złożyć nie później niż do dnia **10.02.2020 roku do godz. 09 [00]**
2. Otwarcie ofert odbędzie się w dniu **10.02.2020 r. o godz. 09:05**
3. Zamawiający zastrzega sobie prawo przesunięcia terminu składania i otwarcia ofert.

9. Termin związania ofertą

1. Termin związania ofertą wynosi 30 dni od upływu terminu składania ofert.
2. Wykonawca, który złożył ofertę najkorzystniejszą będzie zobowiązany do podpisania umowy wg wzoru (załącznik nr 4) przedstawionego przez Zamawiającego i na określonych w niej warunkach, w miejscu i terminie wyznaczonym przez Zamawiającego.

Załączniki:

a) załącznik nr 1 –Formularz ofertowy
b) załącznik nr 2- Szczegółowy opis przedmiotu zamówienia
c) załącznik nr 3 - Oświadczenie
d) załącznik nr 4 – Wzór umowy
e) załącznik nr 5 – informacja RODO

Załącznik nr 1 do zapytania ofertowego

FORMULARZ OFERTOWY

Przedmiot zamówienia	**„FORTIGATE 300C „**
Zamawiający	***Szpital Specjalistyczny w Pile im. Stanisława Staszica 64–920 Piła, ul. Rydygiera 1***
Oferent – pełna nazwa Oferenta, ***adres,*** ***tel., fax.*** ***NIP*** ***REGON*** ***e-mail***	
Oferowana wartość za wykonanie zadanie *(podlega ocenie)*	**wartość netto:…….** **słownie: ……..** **stawka VAT: ……..** **wartość brutto: …….**
Termin płatności	**60 dni**
Termin realizacji zamówienia	**20.02.2020**
Imiona, Nazwiska, osób upoważnionych do podpisania umowy (zgodnie z ustanowioną zasadą reprezentacji)	

ZOBOWIĄZANIA W PRZYPADKU PRZYZNANIA ZAMÓWIENIA:

1) zobowiązujemy się do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego;
2) osoby które będą zawierały umowę ze strony Wykonawcy:

.....

e-mail:……tel.....;

3) osobą odpowiedzialną za realizację umowy jest:

.....

e-mail:……tel.....;

oświadczam, że:

Oświadczamy, że zapoznaliśmy się z opisem przedmiotu zamówienia i nie wnosimy do niego żadnych uwag oraz uzyskaliśmy konieczne informacje i wyjaśnienia niezbędne do przygotowania oferty.

Oświadczamy, że czujemy się związani ofertą na czas wskazany w zapytaniu ofertowym istotnych warunków zamówienia, tj. przez okres 30 dni, licząc od upływu składania ofert.

Oświadczamy, że zapoznaliśmy się z projektem umowy i nie wnosimy zastrzeżeń, co do jej treści.

Oświadczamy, że zapoznaliśmy się z informacją RODO i Instrukcją bezpieczeństwa i higieny prac realizowanych przez podmioty zewnętrzne na terenie Szpitala Specjalistycznego w Pile im. Stanisława Staszica .

Oświadczamy, że cena brutto podana w niniejszym formularzu zawiera wszystkie koszty wykonania zamówienia, jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty.

Oświadczamy, iż powyższe zamówienie w całości zrealizujemy sami.

Załącznikami do niniejszej oferty są:

1. ……..
2. ……..
3. ……..
4. ……..
5. ……..
6. ……..

Oferta została złożona na ..... zapisanych i kolejno ponumerowanych oraz podpisanych stronach.

..... dnia ..... ……..

podpis osoby uprawnionej do składania oświadczeń woli w imieniu Wykonawcy

Przedmiotem zamówienia jest zakup oraz wymiana sprzętu zapory sieciowej tzw. Firewall wraz z oprogramowaniem dla Szpitala Specjalistycznego w Pile im. Stanisława Staszica

Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest wymiana urządzenia firmy Fortinet wchodzącego w skład infrastruktury sieciowej i bezpieczeństwa Zamawiającego tj. w Szpitalu Specjalistycznym w Pile im. Stanisława Staszica 64-920 Piła ul. Rydygiera 1 wraz z usługą wymiany i przeniesienia konfiguracji z urządzeń podlegających wymianie.

Zamawiający posiada następujące urządzenie podlegające wymianie: FortiGate 300C – 1 szt.

Szczegółowe dane urządzeń:

Producent	**Model**	**Numer Seryjny**
Fortinet	FortiGate300C	FG300C3913605610

Zamawiający posiada również 60 szt. bezprzewodowych punktów dostępowych FAP-221C, dla których urządzenie FortiGate 300C pełni funkcję kontrolera bezprzewodowego. Po wymianie urządzeń na nowe funkcjonalność ta musi zostać zachowana.

Powyższe urządzenie użytkowane jest w siedzibie Zamawiającego. Dostarczone urządzenie musi zostać w pełni skonfigurowane na miejscu w siedzibie Zamawiającego przez osoby wyznaczone przez Wykonawcę do realizacji zamówienia.

Po wymianie, urządzenie musispełniać następujące minimalne parametry techniczne:

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, IPSecVPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 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. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. 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:
   - 18 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 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 musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 4 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 32 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 7 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 15 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3.9 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 StatefulInspection.
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 -IntrusionPrevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Trafficshaping).
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) dlaprotokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

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/CounterMode(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.

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.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

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.

Kontrola Antywirusowa

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.

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 6500 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 2500 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. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

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.

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. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
- ICSA dla funkcji SSL VPN.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) 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 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2. <u>Opisy do wymagań ogólnych:</u>

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

OŚWIADCZENIE WYKONAWCY O SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU

oświadczam, że:

1) *Posiadam uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania*
2) *Posiadam wiedzę i doświadczenie,*
3) *Dysponuję odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia,*
4) *Znajduję się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.*
5) *Zapoznaliśmy się ze zapytaniem ofertowym oraz wzorem umowy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte;*
6) *uzyskaliśmy konieczne informacje i wyjaśnienia niezbędne do przygotowania oferty,*
7) *posiadamy status Autoryzowanego Partnera Fortinet,*
8) *Zapoznaliśmy się z załącznikiem nr 2 do zapytania ofertowego, nie wnosimy zastrzeżeń oraz przyjmujemy warunki w nim zawarte;*

Załącznik nr 4 do zapytania ofertowego
Umowa - Projekt

UMOWA Nr …..2020/ZP
zawarta w Pile w dniu ..... 2020 roku

pomiędzy:
Szpitalem Specjalistycznym w Pile im. Stanisława Staszica
64-920 Piła, ul. Rydygiera 1
wpisanym do Krajowego Rejestru Sądowego KRS 0000008246 - Sąd Rejonowy Nowe Miasto i Wilda w Poznaniu, IX Wydział Gospodarczy Krajowego Rejestru Sądowego
REGON: 001261820 NIP: 764-20-88-098
który reprezentuje:
Wojciech Szafrański – Dyrektor
zwanym dalej „Zamawiającym"
a
……
……
wpisanym do Krajowego Rejestru Sądowego KRS …….. – Sąd Rejonowy w ……, ….. Wydział Gospodarczy Krajowego Rejestru Sądowego,
REGON: ..... NIP: .....
który reprezentuje:
……
wpisanym do rejestru osób fizycznych prowadzących działalność gospodarczą Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej (CEIDG)
REGON: ..... NIP: .....
który reprezentuje:
……
zwanym dalej „Wykonawcą", którego oferta została przyjęta w postępowaniu o udzielenie zamówienia publicznego na § 8 Regulaminu udzielania zamówień publicznych, który stanowi załącznik do zarządzenia nr 67/2019 Dyrektora Szpitala Specjalistycznego w Pile im. Stanisława Staszica z dnia 08.05.2019 r. prowadzonego pod hasłem **„FORTIGATE 300C" II** (nr sprawy: EZP-.IV-240/15/20/ZO), o następującej treści:

§ 1

1. W ramach przedmiotu umowy Wykonawca zobowiązany jest do dostawy następujących gwarancji, licencji i usługi **zakup oraz wymiana sprzętu zapory sieciowej tzw. Firewall wraz z oprogramowaniem dla Szpitala Specjalistycznego w Pile im. Stanisława Staszica. Wsparcie techniczne i serwisowe.** Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 1 do umowy.
2. Wykonawca zapewni również wsparcie techniczne i serwisowe.
3. Wykonawca powinien zapewnić bezpośrednie (na miejscu w szpitalu) wdrożenie aktualizacji i serwisów podanych w zapytaniu.
4. Ze względu na krytyczny charakter aktualizacji i serwisów ujętych w zapytaniu (brak ich działania może stanowić zagrożenie dla zabezpieczenia i ochrony danych w szpitalu), czas na przywrócenie ich działania po ewentualnej awarii z uwzględnieniem dojazdu do miejsca usunięcia awarii powinna być nie większa niż 2 godziny.
5. Wykonawca powinien posiadać status Autoryzowanego Partnera Forti.
6. Zamawiający nie dopuszcza wykonywania usługi przez podwykonawcę.
7. Wykonawca zrealizuje przedmiot zamówienia określony w pkt. 1 w terminie **do 20 lutego 2020 roku**. Czas trwania usługi określonej w pkt. 5 wynosi **- 12 miesięcy od dnia podpisania umowy.**

§ 2

1. Wykonawca oświadcza, że osoby, które w jego imieniu wykonywać będą umowę, posiadają kwalifikacje i uprawnienia do wykonywania niniejszej umowy. Wykonawca ponosi odpowiedzialność za działania ww. osób, jak za działania własne.
2. Do obowiązku Wykonawcy należy:
   a) wykonanie prac z zachowaniem należytej dbałości o pozostający w jego dostępie sprzęt i wyposażenie Zamawiającego,
   b) przestrzeganie przepisów BHP, p.poż. oraz podporządkowanie się przekazanym regulaminom i zarządzeniom obowiązującym u Zamawiającego,
   c) podporzadkowanie się zaleceniom administratora budynku oraz pracowników Zamawiającego, którzy są odpowiedzialni za realizację umowy,
   d) wykonanie przedmiotu umowy zgodnie z aktualnymi przepisami prawa.
3. Każda wykonana usługa w trakcie okresu gwarancyjnego zostanie potwierdzona protokołem, zawierającym zakres, datę jej wykonania, użyte materiały podpisanym przez osoby upoważnione.
4. Koszty materiałów wynikających z awarii urządzeń w trakcie okresu gwarancyjnego, których napraw dokonał Wykonawca, jak również wszelkie inne koszty związane z usuwaniem awarii ponosi Wykonawca.
5. Zamawiający powierza Wykonawcy do przetwarzania dane osobowe, jedynie w celu i zakresie niezbędnym do właściwego wykonania Umowy.

§ 3

CENA USŁUGI

1. Cena przedmiotu umowy obejmuje wszystkie określone prawem podatki, opłaty celne i graniczne oraz inne koszty związane z realizacją umowy oraz zapewnienie rocznego wparcia technicznego i serwisowego.
2. Wynagrodzenie Wykonawcy za przedmiot umowy zgodnie z złożoną ofertą wynosi:
   netto: ..... (słownie: .....)
   VAT: .....
   brutto: ..... (słownie: .....)

§ 4

WARUNKI PŁATNOŚCI

1. Zapłata nastąpi na podstawie faktury wystawionej przez Wykonawcę i podpisanego protokołu odbioru przez obie Strony Umowy.
2. Zapłata nastąpi przelewem na konto Wykonawcy nie później niż w ciągu 60 dni od daty doręczenia faktury Zamawiającemu. W przypadku błędnie sporządzonej faktury VAT w tym braku na fakturze zapisów, o mowa w § 9 niniejszej umowy, termin płatności ulegnie odpowiedniemu przesunięciu o czas, w którym doręczono prawidłowo sporządzoną fakturę.
3. Za datę zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.

§ 5

Przedstawicielem Zamawiającego odpowiedzialnym za prawidłowe wykonanie przedmiotu umowy jest Kierownik Działu Informatyki, tel. 67 2106 600

§ 6

KARY UMOWNE

1. W razie odstąpienia od umowy z winy Wykonawcy, zobowiązany jest on zapłacić Zamawiającemu karę umowną w wysokości 20% wartości brutto części niezrealizowanej umowy.
2. W razie opóźnienia w wykonaniu umowy Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,5% wartości brutto umowy, za każdy dzień opóźnienia od terminu wskazanego w §1 ust. 3.
3. Jeżeli wysokość szkody przekracza wysokość kary umownej, Zamawiający zastrzega sobie prawo dochodzenia na drodze sądowej odszkodowania przekraczającego wysokość kary.

§ 7

1. Zamawiający może odstąpić od umowy, z przyczyn leżących po stronie Wykonawcy w szczególności w przypadkach:
   a) nienależytego wykonywania postanowień niniejszej umowy,
   b) stwierdzenie przez Zamawiającego wady fizycznej lub prawnej przedmiotu umowy.
2. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim przypadku Wykonawca może żądać jedynie wynagrodzenia należnego z tytułu wykonania części umowy.

§ 8

1. Zmiana postanowień niniejszej umowy może nastąpić za zgodą obu stron wyrażoną na piśmie pod rygorem nieważności z zastrzeżeniem ust. 2.
2. Niedopuszczalna jest zmiana postanowień niniejszej umowy w stosunku do treści oferty na podstawie, której dokonano wyboru Wykonawcy chyba, że konieczność wprowadzenia takich zmian wynika z uwarunkowań zewnętrznych niezależnych od stron umowy, a zmiana jest nieistotna w stosunku do treści oferty.
3. Zamawiający dopuszcza możliwość zmiany zapisów umowy w następującym zakresie:
   a) zmiany terminu realizacji zamówienia w sytuacji, gdy zmiana ta wynika z przyczyn niezależnych od Wykonawcy;
   b) działania sił wyższych uniemożliwiających wykonanie umowy w określonym pierwotnym terminie;
   c) zmian wynikających z przekształceń własnościowych,
   d) zwiększenia o mniej niż 10% kwoty maksymalnego zobowiązania Zamawiającego, o której mowa w § 3 ust. 2 Umowy.
4. Wykonawca zobowiązany jest do poinformowania Zamawiającego o wszystkich zdarzeniach mających lub mogących mieć wpływ na wykonanie umowy.

§ 9

Wykonawca zobowiązany jest umieścić na fakturze zapis: „Wierzytelności, jakie mogą powstać przy realizacji niniejszej umowy u Wykonawcy w stosunku do Zamawiającego nie mogą być przedmiotem ich dalszej sprzedaży, jak również cesji lub przelewu bez pisemnej zgody Zamawiającego” oraz zapis: „Usługa dotyczy wykonania umowy nr …../2020/ZP z dnia …….”

§ 10

W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy kodeksu cywilnego oraz inne obowiązujące przepisy prawne.

§ 11

Ewentualne spory wynikłe na tle realizacji niniejszej umowy rozstrzygać będzie sąd właściwy miejscowo dla siedziby Zamawiającego, po uprzednim dążeniu stron do ugodowego załatwienia sporu.

§ 12

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

WYKONAWCA ZAMAWIAJĄCY

Załącznik nr 1 do Umowy

Przedmiotem zamówienia jest zakup oraz wymiana sprzętu zapory sieciowej tzw. Firewall wraz z oprogramowaniem dla Szpitala Specjalistycznego w Pile im. Stanisława Staszica

Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest wymiana urządzenia firmy Fortine twchodzącego w skład infrastruktury sieciowej i bezpieczeństwa Zamawiającego tj.w Szpitalu Specjalistycznym w Pile im. Stanisława Staszica 64-920 Piła ul. Rydygiera 1 wraz z usługą wymiany i przeniesienia konfiguracji z urządzeń podlegających wymianie.

Zamawiający posiada następując eurządzenie podlegające wymianie: FortiGate 300C – 1 szt.

Szczegółowe dane urządzeń:

Producent	**Model**	**Numer Seryjny**
Fortinet	FortiGate300C	FG300C3913605610

Zamawiający posiada również 60 szt. bezprzewodowych punktów dostępowych FAP-221C, dla których urządzenie FortiGate 300C pełni funkcję kontrolera bezprzewodowego. Po wymianie urządzeń na nowe funkcjonalność ta musi zostać zachowana.

Powyższe urządzenie użytkowanejest w siedzibie Zamawiającego. Dostarczone urządzenie musi zostać w pełni skonfigurowane na miejscu w siedzibie Zamawiającego przez osoby wyznaczone przez Wykonawcę do realizacji zamówienia.

Po wymianie, urządzenie musi spełniać następujące minimalne parametry techniczne:

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, IPSecVPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 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

6. 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.

7. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
8. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
9. Monitoring stanu realizowanych połączeń VPN.
10. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

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

Parametry wydajnościowe:

8. W zakresie Firewall'a obsługa nie mniej niż 4 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę.
9. Przepustowość Stateful Firewall: nie mniej niż 32 Gbps.
10. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 7 Gbps.
11. Wydajność szyfrowania IPSec VPN: nie mniej niż 15 Gbps.
12. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
13. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
14. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3.9 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:

13. Kontrola dostępu - zapora ogniowa klasy StatefulInspection.
14. Kontrola Aplikacji.
15. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
16. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
17. Ochrona przed atakami -IntrusionPrevention System.
18. Kontrola stron WWW.
19. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
20. Zarządzanie pasmem (QoS, Trafficshaping).
21. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
22. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokenysprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
23. Analiza ruchu szyfrowanego protokołem SSL.
24. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

4. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
5. 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) dlaprotokołu SIP.

6. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

3. 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/CounterMode(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.
4. 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.

Routing i obsługa łączy WAN

3. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
4. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

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

Kontrola Antywirusowa

5. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
6. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
7. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
8. 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.

Ochrona przed atakami

8. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

9. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
10. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
11. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
12. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
13. 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.
14. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

6. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
7. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
8. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
9. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
10. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

6. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
7. 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.
8. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
9. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
10. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

4. 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.
5. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
6. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

7. 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.
8. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
9. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
10. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

11. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
12. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

4. 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.
5. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
6. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
- ICSA dla funkcji SSL VPN.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) 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 12 miesięcy.

Gwarancja oraz wsparcie

3. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

4. <u>Opisy do wymagań ogólnych:</u>

3. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
4. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Załącznik nr 2 do Umowy

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

stanowiąca uzupełnienie umowy nr…… **z dnia …… r.**

zawarta w dniu …….. r. w Pile,

zwana dalej „Umową powierzenia"

pomiędzy:
Szpitalem Specjalistycznym w Pile im. Stanisława Staszica
ul. Rydygiera 1
64-920 Piła
wpisanym do Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Poznań Nowe Miasto i Wilda, IX Wydział Gospodarczy pod numerem
KRS: **0000008246**
numer NIP: **764-20-88-098** REGON: **001261820**
reprezentowanym przez
Dyrektora – Wojciecha Szafrańskiego
zwany dalej **„Zamawiającym"**

oraz:
……
……, ul. ……..
wpisaną do KRS pod nr ……..

reprezentowanym przez

……..

zwaną dalej **„Zleceniobiorcą"**
Strony zawierają Umowę powierzenia przetwarzania danych osobowych o treści jak poniżej.

§ 1

Przedmiot przetwarzania

1. Strony zawarły Umowę nr …….. z dnia …….. 20……. r. na zakup oraz wymianę sprzętu zapory sieciowej tzw. Firewall wraz z oprogramowaniem dla Szpitala Specjalistycznego w Pile im. Stanisława Staszica". Wsparcie techniczne I serwisowe. Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 1 do Umowy Podstawowej. W celu jej realizacji niezbędne jest powierzenie przetwarzania danych osobowych Przetwarzającemu.
2. Zleceniodawca oświadcza, ze jest Administratorem danych osobowych, które powierza Przetwarzającemu do przetwarzania.
3. W ramach Umowy Zleceniodawca powierza Zleceniobiorcy zgodnie z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, czynności związane z przetwarzaniem dalej szczegółowo opisanych danych osobowych wyłącznie w celu realizacji Umowy Podstawowej.
4. Dane osobowe przetwarzane będą przez Zleceniobiorcę wyłącznie w zakresie i celu niezbędnym do należytego wykonania przez Zleceniobiorcę Umowy Podstawowej.

5. Jakiekolwiek przetwarzanie danych osobowych, o których mowa w Umowie poza tym zakresem i celem będzie działaniem wbrew upoważnieniu Zleceniodawcy.
6. Zleceniobiorca będzie przetwarzał powierzone dane osobowe, na podstawie Umowy powierzenia, w tym dane szczególnej kategorii zapisane w programach wymienionych w § 2 pkt 2 dot. pacjentów, osób upoważnionych przez pacjentów i personelu szpitala i ich rodzin, kontrahentów, osób odbywających naukę zawodu,
7. Postanowienia niniejszej Umowy powierzenia pozostają w pełni zgodne z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO").

§ 2

Zasady przetwarzania danych

1. Dane osobowe w zależności od potrzeb będą przetwarzane przez Zleceniobiorcę w siedzibie Zamawiającego lub w siedzibie Zleceniobiorcy. Po wykonaniu czynności serwisowych, o których mowa w § 1 ust. 1 niniejszej Umowy powierzenia, Zleceniobiorca niezwłocznie zobowiązuje się usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w dyspozycji Zleceniobiorcy.
2. Zleceniodawca udziela Zleceniobiorcy dostępu do systemów drogą elektroniczną. Każdy z serwisantów Zleceniobiorcy ma zdefiniowany szyfrowany kanał VPN, którym łączy się ze szpitalem.
3. Każdorazowo zestawione połączenie będzie ewidencjonowane przez Dział Informatyki Zleceniodawcy w dzienniku połączeń: „**Ewidencja zdalnych połączeń w Szpitalu Specjalistycznym w Pile"** na podstawie cotygodniowego raportu „Security Analysis" generowanego przez urządzenie Forti Analyzer.
4. Do wykonania usług serwisowych mogą być dopuszczeni jedynie ci pracownicy Zleceniobiorcy, którzy posiadają imienne upoważnienia do przetwarzania danych osobowych. Pod pojęciem „pracownika" rozumie się osobę świadczącą pracę na podstawie stosunku pracy lub stosunku cywilnoprawnego.
5. Zamawiający udziela Zleceniobiorcy umocowania do wydawania i odwoływania jego pracownikom imiennych upoważnień do przetwarzania danych osobowych. Upoważnienia przechowuje Zleceniobiorca w swojej siedzibie.
6. Zleceniobiorca przekazuje Zleceniodawcy aktualny imienny wykaz osób upoważnionych do przetwarzania danych osobowych.
7. Wszelkie decyzje dotyczące przetwarzania danych osobowych, odbiegających od ustaleń zawartych w niniejszej umowie, powinny być przekazywane drugiej stronie w formie pisemnej pod rygorem ich nieważności.

§ 3

Zabezpieczenie przetwarzanych danych osobowych

1. Zleceniobiorca oświadcza, ze podejmie środki zabezpieczające, wymagane na mocy art. 32 RODO, zgodnie z art. 28 ust. 3 lit. c RODO.
2. Zleceniobiorca oświadcza, ze uwzględniając stan wiedzy technicznej, koszt wdrażania oraz **charakter,** zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia zastosowane środki techniczne i organizacyjne, są odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku przetwarzania Powierzonych Danych, tj.
    a) prowadzi dokumentacją opisującą sposób przetwarzania danych osobowych,
    b) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zabezpieczone są zgodnie z obowiązującymi dobrymi

praktykami w zakresie ochrony infrastruktury i zasobów teleinformatycznych jak również, że zabezpieczenia te pozostają w zgodzie z obowiązującymi przepisami prawa, w tym szczególności szyfruje Powierzone Dane,

c) stosuje odpowiednie środki techniczne i organizacyjne do zapewnienia przetwarzanym w ramach jego umowy danym ochrony, w szczególności zabezpiecza dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO, zmianą, utratą, uszkodzeniem lub zniszczeniem.

§4

Współdziałanie w wykonywaniu praw osób, których dane dotyczą

1. Zleceniobiorca wdroży odpowiednie środki techniczne i organizacyjne, aby móc wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO, w szczególności w zakresie zagwarantowania:
   a) prawa do wglądu do swoich danych osobowych,
   b) prawa do sprostowania danych,
   c) prawa do usunięcia danych,
   d) prawa do sprzeciwu,
   e) oraz prawa do przenoszenia danych.
2. Zleceniobiorca zobowiązuje się do przekazywania Zleceniodawcy żądanych przez podmiot informacji/podejmowania określonych działań niezwłocznie, ale nie później, niż w terminie 7 dni od dnia poinformowania Zleceniobiorcę przez Zleceniodawcę o wystąpieniu do Przetwarzającego z takim wnioskiem przez podmiot danych, a także zobowiązuje się współpracować z Zleceniodawcą w miarę możliwości w celu jego realizacji.

§5

Zarejestrowanie i zgłoszenie incydentu

1. Zgodnie z art. 28 ust. 3 lit. f RODO, Zleceniobiorca uczestniczy w realizacji obowiązku Zleceniodawcy, określonego w art. 33 RODO, w szczególności niezwłocznie, nie później niż w ciągu 24 godzin poinformuje Inspektora Ochrony Danych lub *osobę* odpowiedzialną za ochronę danych u Zleceniodawcy o jakichkolwiek przypadkach naruszenia ochrony danych osobowych tzw. incydentach wraz z:

a. opisem charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazaniem kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

b. opisem możliwych konsekwencji naruszenia ochrony danych osobowych,

c. opisem zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

2. W przypadku, gdy ustalenie wszelkich danych dotyczących incydentu będzie niemożliwe w terminie wskazanym w ust. 1, Zleceniobiorca będzie przekazywał informacje sukcesywnie, w miarę ich pozyskiwania.
3. Zleceniobiorca prowadzi bieżącą dokumentację zawierającą opis naruszeń, o których mowa w ust. 1 powyżej. Na żądanie Zleceniodawcy niezwłocznie, nie później niż w ciągu 24 godzin przekaże kopię prowadzonej dokumentacji.
4. Na żądanie Zleceniodawcy Zleceniobiorca zobowiązuje *się*udzielić wszelkich informacji dotyczących Przetwarzanych Danych w sytuacji, powzięcia informacji o wystąpieniu

incydentu przez Zleceniodawcę od osoby trzeciej niezwłocznie, nie później niż w ciągu 24 godzin.

§ 6
Kontrola zabezpieczeń

1. Zleceniodawca zastrzega sobie możliwość kontroli sposobu wypełnienia przez Zleceniobiorcę obowiązków umownych, zgodnie z art. 28 ust. 3 lit. h RODO.
2. Zleceniodawca jest uprawniony do żądania udzielania informacji lub wyjaśnień w formie pisemnej, w postaci papierowej lub elektronicznej, dotyczących Powierzonych Danych. Zleceniobiorca jest zobligowany udzielić wszelkich niezbędnych informacji dotyczących realizacji postanowień Umowy niezwłocznie, nie później niż 7 dni od dnia otrzymania żądania.
3. W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Zleceniodawcy za przetwarzanie Powierzonych Danych, Zleceniobiorca zobowiązany jest niezwłocznie podjąć działania w celu ich usunięcia oraz natychmiast poinformować o nich Zleceniodawcę.
4. Zleceniobiorca niezwłocznie informuje Zleceniodawcę o wszelkich czynnościach, w szczególności kontrolnych i skargowych, prowadzonych przez organ nadzorczy z zakresu Powierzonych Danych jeśli przepis prawa nie zabrania podania takich danych.
5. Zleceniodawca zastrzega sobie prawo do kontroli zgodności przetwarzania Powierzonych Danych z niniejszą Umową przez Zleceniobiorcę. Zleceniodawca powiadomi Zleceniobiorcę o zamiarze przeprowadzenia przedmiotowej kontroli z wyprzedzeniem, nie krótszym niż 7 dni. Zleceniobiorca zobowiązany jest umożliwić Zleceniodawcy przeprowadzenie przedmiotowej kontroli, w szczególności poprzez udostępnienie systemów informatycznych, nośników, dokumentacji i pomieszczeń, w zakresie niezbędnym dla kontroli przetwarzania Powierzonych Danych.
6. W przypadku powzięcia przez Zleceniodawcę wiadomości o rażącym naruszeniu zobowiązań wynikających z przepisów obowiązującego prawa lub Umowy, a także incydencie, Zleceniobiorca umożliwi Zleceniodawcy przeprowadzenie niezapowiedzianej kontroli.
7. Zleceniobiorca jest zobowiązany do zastosowania się do zaleceń pokontrolnych sformułowanych przez Zleceniodawcę dotyczących zabezpieczenia Powierzonych Danych.

§ 7
Współdziałanie przy kontroli organu nadzorczego

1. Zleceniobiorca zobowiązuje się współdziałać z Zleceniodawcą w przypadku wszczęcia przez organ nadzorczy postępowania kontrolnego u Zleceniodawcy, o ile w zakresie kontroli będą również Powierzone Dane.
2. Na żądanie Zleceniodawcy Zleceniobiorca stawi się w wyznaczonym na przeprowadzenie kontroli miejscu i czasie.

§8
Odpowiedzialność i prawo do odszkodowania

1. Zleceniobiorca jest w pełni odpowiedzialny za udostępnienie lub wykorzystanie Powierzonych Danych niezgodnie z treścią Umowy, a w szczególności za udostępnienie Powierzonych Danych osobom nieupoważnionym.
2. Zleceniodawca odpowiada za szkody spowodowane przetwarzaniem gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające, lub gdy podmiot działał poza zgodnymi z prawem instrukcjami Zleceniodawcy lub wbrew tym instrukcjom.

3. Zleceniodawca oraz Zleceniobiorca odpowiadają w stosunku do osób zainteresowanych oraz w stosunku do siebie nawzajem w sposób opisany w art. 82 RODO.
4. W przypadku podniesienia jakichkolwiek roszczeń w rozumieniu art. 82 RODO wobec Zleceniodawcy przez osobę zainteresowaną, Zleceniobiorca zobowiązuje się do wspierania Zleceniodawcę przy obronie przed tymi roszczeniami, na ile będzie to możliwe.
5. W przypadku, w którym Zleceniodawca zostanie zobowiązany prawomocną decyzją lub prawomocnym wyrokiem właściwego sądu do zapłaty kary pieniężnej, odszkodowania, zadośćuczynienia lub jakiejkolwiek innej kwoty z tytułu naruszenia przepisów dotyczących ochrony danych osobowych lub w związku ze szkodą lub krzywdą wyrządzoną w związku z naruszeniem przepisów dotyczących ochrony danych osobowych, jeśli takie naruszenie lub szkoda (krzywda) wynikać będą z naruszenia przez Zleceniobiorcę postanowień Umowy, Zleceniobiorca odpowiada względem Zleceniodawcy w pełnej wysokości, niezależnie od jakichkolwiek ograniczeń odpowiedzialności przewidzianych w Umowie lub Umowie Podstawowej i zobowiązany jest zwrócić Zleceniodawcy wszelkie koszty poniesione przez Zleceniodawcę, w tym w szczególności zwrócić kwotę wypłaconego odszkodowania, zadośćuczynienia lub kary pieniężnej.

§9
Czas obowiązywania umowy

1. Umowa obowiązuje na czas obowiązywania Umowy Podstawowej.
2. Zleceniodawca może wypowiedzieć niniejszą Umowę ze skutkiem natychmiastowym w każdym czasie, w szczególności w sytuacji nieprzestrzegania przez Zleceniobiorcę postanowień Umowy oraz obowiązujących przepisów prawa z zakresu ochrony danych osobowych.
3. Zobowiązanie do zachowania poufności nie wygasa po zakończeniu Umowy i jest nieograniczone w czasie.

§10
Zakończenie przetwarzania danych

Po zakończeniu przetwarzania Powierzonych Danych zgodnie z niniejszą Umową, według wyboru Zleceniodawcy, Zleceniobiorca zobowiązuje się w terminie 7 dni:

1. trwale usunąć Powierzone Dane,
2. zaniechać ich przetwarzania we własnym zakresie, zgodnie z art. 28 ust. 3 lit. g RODO,

chyba ze prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania tychże danych osobowych.

§11
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
2. Prawem właściwym dla Umowy jest prawo Rzeczpospolitej Polskiej.
3. Zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Wszelkie spory wynikające z niniejszej Umowy lub powstające w związku z nią będą rozstrzygane przez Sąd właściwy miejscowo dla Zleceniodawcy.

Zamawiający **Zleceniobiorca**

Informacja RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

a) **administratorem Pani/Pana danych osobowych jest Szpital Specjalistyczny w Pile im. Stanisława Staszica, ul. Rydygiera 1; 64-920 Piła**
b) inspektorem ochrony danych osobowych w Szpitalu jest Pan Piotr Musiał, kontakt: tel. 67 2106295, e-mail: iod@szpitalpila.pl, siedziba: pokój H021 na niskim parterze budynku „H";
c) Pani/Pana dane osobowe przetwarzane będą w celu związanym z postępowaniem o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego;
d) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp";
e) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, 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, umowy 10 lat od dnia rozwiązania umowy;
f) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
g) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
h) posiada Pani/Pan:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych[1];
   - 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[2];
   - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
i) 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.

[1] Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników

[2] Wyjaśnienie: 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.