ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa zamówienia

Rozbudowa infrastruktury „F5 BIG-IP" wraz z dostawą stacji roboczych i monitorów.

II. Kody CPV

32424000-1 - Infrastruktura sieciowa
30231300-0 - Monitory ekranowe
30214000-2 - Stacje robocze

III. Przedmiot zamówienia

Przedmiotem zamówienia jest dostarczenie licencji pozwalającej na uruchomienie funkcjonalności WAF, w celu rozbudowy posiadanej przez Zamawiającego infrastruktury F5 BIG-IP 5000s lub dostarczenie licencji równoważnych oraz dostawa stacji roboczych i monitorów.

Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji:

Nazwa / skrót	Opis
Dzień Roboczy	Oznacza dzień od poniedziałku do piątku niebędący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.
Osobodzień	Oznacza jednostkę miary czasu wykonywania usług, obejmującą pracę jednej osoby przez 8 godzin, bez ograniczenia Dni Roboczych.
Wsparcie producenta	Oznacza oferowane przez producenta danego rozwiązania aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane dla poszczególnych urządzeń przez zdefiniowany okres czasu.
WAF	Ang. Web Application Firewall oznacza moduł ochrony ruchu webowego realizowany w Urządzeniu F5 BIG-IP 5000s posiadanym przez Zamawiającego.
Infrastruktura Zamawiającego	Oznacza dwa urządzenia F5 BIG-IP 5000s, posiadane przez Zamawiającego, opisane przez Zamawiającego w oświadczeniu, przekazywanym Wykonawcom zgodnie z postanowieniami ust. 4 pkt 4.2. Rozdziału I SIWZ .

1. W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co mogłoby prowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne". Nie dotyczy to sytuacji, w których Zamawiający definiuje posiadaną przez siebie infrastrukturę w celu precyzyjnego określenia środowiska, z którym przedmiot zamówienia ma być kompatybilny.

2. W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na normy, europejskie oceny techniczne, aprobaty, specyfikacje techniczne i systemy referencji technicznych, należy odczytywać z wyrazami „lub równoważne". Nie dotyczy to sytuacji, w których Zamawiający definiuje posiadaną przez siebie infrastrukturę w celu precyzyjnego określenia środowiska, z którym przedmiot zamówienia ma być kompatybilny.
3. W przypadku zaoferowania rozwiązania równoważnego, zgodnie z art. 30 ust. 5 ustawy Pzp, na Wykonawcy spoczywa obowiązek wykazania jego równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez urządzenia lub oprogramowanie równoważne poszczególnych parametrów równoważności. Zamawiający wymaga realizacji takiego obowiązku w ofercie Wykonawcy.
4. Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.
5. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury u Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu oprogramowania.

III.1 Rozbudowa infrastruktury F5 BIG-IP 5000s

1. Przedmiotem zamówienia jest dostawa odpowiednich dwóch licencji pozwalających uruchomić funkcjonalność WAF dla dwóch urządzeń producenta F5 z serii BIG-IP 5000s, które Zamawiający posiada w swojej Infrastrukturze.
2. Zamawiający przekaże informacje dotyczące aktualnie wykorzystywanej Infrastruktury Zamawiającego, obejmujące Serial Number dwóch urządzeń wchodzących w skład tej infrastruktury, Wykonawcom, którzy złożą do Zamawiającego wniosek o udostepnienie takich informacji, zgodnie z procedurą opisana w ust. 4 pkt. 4.2. Rozdziału I SIWZ, obejmującą między innymi: złożenie wniosku w formie elektronicznej, wg wzoru przygotowanego przez Zamawiającego, złożenie oświadczenia o zachowaniu poufności wg wzoru przygotowanego przez Zamawiającego, udostępnienie przez Zamawiającego informacji poprzez wysłanie zaszyfrowanego dokumentu za pośrednictwem poczty elektronicznej oraz hasła za pośrednictwem wiadomości SMS.
3. W związku z uruchomieniem tej funkcjonalności, przedmiot zamówienia obejmuje dostawę dwóch licencji (pkt III.1.1.), świadczenie usług profesjonalnych (pkt III.1.2.) oraz realizację szkoleń dotyczących przedmiotu zamówienia (pkt III.1.3.).

III.1.1 DOSTAWA LICENCJI WAF

1. W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy licencje konieczne do uruchomienia funkcjonalności Web Application Firewall (zwanej dalej „WAF"), w najszerszym przewidzianym przez producenta zakresie na dwóch urządzeniach F5 BIG-IP 5000s, które posiada Zamawiający.
2. Zamawiający wymaga dostarczenia w/w licencji wraz ze wsparciem producenta lub podmiotu autoryzowanego przez producenta, działającego w imieniu producenta na okres nie krótszy niż 3 lata od daty podpisania protokołu odbioru licencji, umożliwiającym składanie zgłoszeń serwisowych i korzystanie z aktualizacji sygnatur oraz baz wiedzy udostępnianych przez producenta w tym okresie.
3. Oferowana licencja nie może znajdować się w statusie końca sprzedaży (EoS – ang. End of Sale) tak, że data EoS nie może przypadać w pierwszej połowie 2021 roku lub wcześniej.

Licencje równoważne:

4. Zamawiający dopuszcza jako „licencje równoważne" licencje zapewniające bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanego środowiska zbudowanego w oparciu o licencje wymienione powyżej. Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania opisane poniżej. Nie jest możliwe dostarczenie nowego sprzętu jako rozwiązania równoważnego.

   Licencje równoważne (dwie sztuki) muszą zapewnić (rozszerzenie dotychczasowych funkcjonalności zawartych w dwóch obecnie znajdujących się w infrastrukturze Zamawiającego urządzeniach F5 BIG-IP 5000s):

   (a) możliwość stosowania ochrony przed atakami na aplikacje internetowe i serwery WWW.

   (b) Klucze prywatne (PKI) zapisane na dysku muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.

   (c) WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Pozytywny model bezpieczeństwa musi kontrolować co najmniej:

      i. wystąpienie URL-i, długość URL-i, zabezpieczenie przed tzw.clickjackiem dla danego URL-a.
      ii. typ serwletu występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT)
      iii. przejścia pomiędzy URL-ami (servletami)
      iv. dopuszczalne metody http

v. dopuszczalne cookie
vi. dopuszczalne parametry w polityce
vii. parametry dynamiczne
viii. typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany)
ix. oraz dopuszczalne parametry w danym serwlecie
x. długość zapytań
xi. nazwy hosta
xii. wystąpień i długość parametrów (per każdy parametr)
xiii. wystąpień i długości nagłówków
xiv. wystąpień i długości cookies
xv. oczekiwanych typów znaków per każdy parametr
xvi. typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku
xvii. URL-i podatnych na CSRF

(d) Musi umożliwić profilowanie chronionej / monitorowanej aplikacji web, profilowanie musi być tworzony na podstawie analizy ruchu sieciowego.

(e) WAF musi umożliwiać definiowania dopuszczalnego przepływu sekwencji zapytań w obrębie aplikacji z uwzględnieniem jej logiki biznesowej.

(f) Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń).

(g) Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na podstawie analizy ruchu sieciowego. Algorytmy tworzenia profilu bezpieczeństwa WAF muszą odrzucać nadużycia w procesie nauki.

(h) Musi istnieć możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa.

(i) Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa.

(j) Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http.

(k) WAF musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force.

(l) WAF musi posiadać mechanizmy ochrony przed atakami:

a. SQL Injection
b. Cross-Site Scripting
c. Cross-Site Request Forgery

d. Session hijacking
e. Command Injection
f. Cookie/Session Poisoning
g. Parameter/Form Tampering
h. Forceful Browsing
i. Brute Force Login
j. Web Scraping
k. Cookie manipulation/poisoning
l. Dynamic Parameter tampering
m. Buffer Overflow
n. Stealth Commanding
o. Unused HTTP Methods
p. Malicious File Uploads
q. Hidden Field Manipulation.

(m) Mechanizm zabezpieczenia przed manipulacją cookie serwera aplikacyjnego musi być oparty o wstrzykiwanie cookie z podpisem oryginalnego cookie aplikacji.

(n) WAF musi posiadać mechanizmy ochrony przed atakami DDoS lub DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http).

(o) WAF musi blokować ataki typu Slow Loris.

(p) WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku DDoS lub DoS poprzez wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania mechanizmu browser fingerprinting, w celu wykrycia tzw. headless broser Sygnatury botów oraz wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik).

(q) WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania dużej ilości incydentów wykonywanych w zdefiniowanym czasie przez tego użytkownika.

(r) WAF musi umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania; bez uszczerbku na wydajności WAF-a.

(s) WAF musi umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack-iem.

(t) WAF musi umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny; bez uszczerbku na wydajności WAF-a.

(u) W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP, SMTP oraz FTP.

(v) WAF musi posiadać wsparcie dla aplikacji działających w technologiach AJAX oraz JSON.

(w) WAF musi wyświetlać strony blokowania (błędu) w technologiach AJAX i JSON.

(x) WAF musi posiadać wsparcie dla Google Web Toolkit.

(y) WAF musi posiadać możliwość ochrony komunikacji XML poprzez:

(i) - Walidację Schema/WSDL
(ii) - Wybór dozwolonych metod SOAP
(iii) - Szyfrację /deszyfrację fragmentów wiadomości SOAP
(iv) Wsparcie dla WS-Security (szyfracja, deszyfracja, veryfikacja i podpisywanie)
(v) Definiowanie możliwości użycia załączników wiadomości SOAP
(vi) Włączanie/wyłączanie podążania za odnośnikami do schematów SOAP
(vii) Walidację SOAPAction Header
(viii) Włączanie/wyłączanie możliwości użycia zewnętrznych referencji
(ix) Włączanie/wyłączanie możliwości użycia początkowych białych znaków
(x) Włączanie/wyłączanie możliwości użycia numerycznych nazw
(xi) Włączanie/wyłączanie możliwości użycia Processing Instructions
(xii) Ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace
(xiii) Ograniczenia ilości: zagnieżdżeń w dokumencie, dzieci per element, atrybutów per element, deklaracji NameSpace-ów
(xiv) Definicję dopuszczalnych znaków
(xv) Definicję sygnatur

(z) WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej muszą być dostępne w ramach tych równoważnych licencji.

(aa) WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać, co najmniej:

(bb) Directory traversal
(cc) Kodowanie typu %u
(dd) Kodowanie typu IIS backslash
(ee) IIS Unicode codepoints
(ff) Bare byte decoding
(gg) Apache whitespace
(hh) Bad unescape
(ii) Wstrzykiwanie komentarzy (np. <!-- -->)

(jj) WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji; oraz dowolne inne ciągi znaków zdefiniowany poprzez wyrażenia regularne.

(kk) WAF musi chronić ruch przesyłany po IPv6.

III.1.2 ZASADY ŚWIADCZENIA USŁUG PROFESJONALNYCH

1. Zamawiający wymaga zapewnienia przez Wykonawcę Usług Profesjonalnych świadczonych bezpośrednio przez producenta przedmiotu zamówienia opisanego w pkt III.1.1 powyżej (dalej określanego jako „**Producent**") lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta dla rynku geograficznego właściwego dla Zamawiającego lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta (dalej określanego jako „**Partner**") – w wymiarze łącznie 60 Osobodni, przez okres 36 miesięcy od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt III.1.III.1.1 w pkt 2, powyżej.
2. Osoba/y realizująca Usługę Profesjonalną musi być ekspertem w obszarze związanym z WAF na F5 BIG-IP oraz legitymować się ważnym i aktualnym certyfikatem Producenta lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego Producenta.
3. W ramach Usług Profesjonalnych będzie m.in.:
   3.1. Opracowanie i dostarczenie projektu wdrożenia przedmiotu zamówienia, o którym mowa w pkt III.1III.1.1 powyżej oraz związanej z tym wdrożeniem dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Usług Profesjonalnych;
   3.2. Opracowanie i dostarczenie procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów;
   3.3. Wsparcie we wdrożeniu i konfiguracji przedmiotu zamówienia, o którym mowa w pkt III.1.III.1.1 powyżej;
   3.4. Konsultacje dot. utrzymania, eksploatowania oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez przedmiot zamówienia, o którym mowa w pkt III.1.1 powyżej;
   3.5. Konsultacje dot. konfiguracji, utrzymania i eksploatowania platformy F5 BIG-IP 5000s, w których będzie implementowany przedmiot zamówienia z pkt. III.1.1.
   3.6. Opracowanie konfiguracji WAF na potrzeby chronionych aplikacji Zamawiającego;
   3.7. Pomoc w implementacji nowych reguł i polityk WAF na potrzeby chronionych przez Zamawiającego aplikacji;
   3.8. Tuning polityk i reguł zaimplementowanych w WAF.
4. Zamawiający wymaga zapewnienia realizacji Usług Profesjonalnych, na podstawie zleceń przekazywanych przez personel Zamawiającego, wskazany w zawartej z wykonawcą Umowie, wskazujących przedmiot zamawianych usług, a Wykonawca będzie zobowiązany zapewnić rozpoczęcie świadczenia takich usług nie później niż w terminie 3 Dni Roboczych od dnia przekazania Wykonawcy zlecenia.

III.1.3 ZASADY ŚWIADCZENIA USŁUG SZKOLENIOWYCH

1. Zamawiający wymaga dostarczenia voucherów uprawniających do przeszkolenia 4 osób z zakresu przedmiotu zamówienia lub w przypadku dostarczenia licencji równoważnej opisanej powyżej, dostarczenia voucherów na szkolenie dla 4 osób w zakresie zgodnym z dostarczoną licencją równoważną. Każdy z voucherów ma uprawniać do odbycia szkolenia dla jednej osoby, niezależnie od terminu wykorzystania pozostałych voucherów.
2. Szkolenie musi obejmować zakres dot.:
    2.1. konfiguracji i administracji przedmiotu zamówienia (WAF) lub równoważne*, trwające min. 4 Dni Robocze,
    2.2. z administracji i konfiguracji platformy BIG-IP F5 trwające min. 2 Dni Robocze

*Zamawiający wskazuje, że w przypadku zaoferowania rozwiązania równoważnego, Wykonawca zobowiązany jest zapewnić szkolenia autoryzowane przez producenta oferowanego rozwiązania, zapewniające uczestnikom wiedzę o konfigurowaniu i administrowaniu WAF w Infrastrukturze Zamawiającego z wykorzystaniem takiego rozwiązania równoważnego.

3. Zamawiający będzie uprawniony do wymagania realizacji takiego szkolenia z możliwością aktywnego udziału uczestników szkolenia.
4. Dostarczone vouchery muszą mieć ważność minimum rok czasu od daty podpisania protokołu odbioru voucherów.
5. Dostarczone vouchery muszą umożliwiać realizację szkoleń w języku polskim.
6. Dostarczone vouchery maja uprawniać do odbycia szkolenia prowadzonego przez producenta Infrastruktury Zamawiającego, (dalej określanego jako „Producent") lub autoryzowany przez Producenta podmiot.
7. Szkolenie może zostać przeprowadzone w częściach wyżej wskazanych w pkt. 2, zorganizowane (zależnie od potrzeb zamawiającego) w ośrodku szkoleniowym w Warszawie lub online.

III.2 Dostawa stacji roboczych i monitorów

1. Wykonawca, na co najmniej 1 Dzień Roboczy przed dostawą, jest zobowiązany do przekazania Zamawiającemu na adres e-mail wskazany przez Zamawiającego w Umowie zestawienia wszystkich dostarczonych urządzeń, zgodnie ze złożoną Ofertą, zawierającego takie informacje jak: producent, typ, model, numer seryjny, okres obowiązywania gwarancji, cenę jednostkową netto, cenę jednostkową brutto.
2. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
3. Dostarczany Sprzęt musi być kompletny, tj.: mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie.
4. Zamawiający nie dopuszcza sprzętu prefabrykowanego, wymagana jest dostawa sprzętu fabrycznie nowego, nieużywanego.

5. Zamawiający może wykonywać uprawnienia z tytułu rękojmi niezależnie od uprawnień wynikających z gwarancji jakości.
6. Wykonawca zobowiązuje się w ramach realizacji przedmiotu zamówienia do dostarczenia Zamawiającemu sprzętu opisanego w OPZ, w terminie maksymalnie 30 Dni Roboczych od daty zawarcia umowy.
7. Sprzęt zostanie dostarczony do siedziby Centralnego Ośrodka Informatyki, mieszczącego się przy ul. Aleje Jerozolimskie 132-136, 02-305 Warszawa; budynek Delta, środkiem transportu, którego waga nie przekracza 6 ton.

III.2.1 SPECYFIKACJA STACJI ROBOCZEJ

Specyfikacja Stacji Roboczej wraz z niezbędnym wyposażeniem – 2 szt.	
Produkt	Stacja robocza klasy PC.
Zestaw	1. Stacja robocza. 2. Klawiatura USB w układzie polski programisty. 3. Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll).
Obudowa	Typu Tower z zasilaczem i przewodem zasilającym;
Procesor	Rodziny x 86, który posiada 8 logicznych rdzeni i jest w stanie zapewnić wydajność procesora na poziomie co najmniej 12377* punktów Passmark CPU Mark, wg zestawienia dla systemów jednoprocesorowych publikowanego przez producenta testu opublikowanego na dzień otwarcia ofert, który dostępny jest na stronie: www.cpubenchmark.net/cpu_list.php.
Pamięć operacyjna RAM	Min. 32 GB – DDR4 ECC. Minimum 4 wolnych banków pamięci na potrzeby przyszłej rozbudowy.
Parametry pamięci masowej	Min. 1 szt. dysk minimum 1 TB 7200 obr./min. plus 1 dysk SSD minimum 250GB z interfejsem PCIe.
Karta graficzna	Umożliwiająca podłączenie minimum 2 monitorów kompatybilna z monitorem wskazanym w niniejszej części dokumentu.
Karta dźwiękowa	Zintegrowana.
Napęd DVD+/-RW	Nie wymagany
System operacyjny	Nie wymagany
Standardy i certyfikaty	Deklaracja zgodności CE dla oferowanego modelu (załączyć przy dostawie).
Złącza	1. Do podłączenia monitora wskazanego w niniejszej części dokumentu – minimum 2 szt.;

Specyfikacja Stacji Roboczej wraz z niezbędnym wyposażeniem – 2 szt.	
	2. Porty USB 3.1 – minimum 2 szt. z przodu obudowy. 3. Porty USB 3.0 – minimum 4 szt. z tyłu obudowy. 4. RJ-45 – 1 szt. (karta sieciowa zintegrowana 1 Gb/s). 5. Zasilanie (AC) – 1 szt.
Zasilanie	Wewnętrzny zasilacz 750 W, sprawność min. 90%, aktywny stabilizator PFC.
BIOS	BIOS w standardzie UEFI musi posiadać następujące cechy: 1. BIOS musi zawierać nieulotną informację z nazwą producenta, nazwą produktu, jego numerem seryjnym, wersji BIOS, a także informację o typie zainstalowanego procesora, ilości i typie pamięci RAM, rodzaju układu graficznego. 2. Informacji o dysku twardym: model oraz pojemność. 3. Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, portów USB z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego stacji roboczej lub innych, podłączonych do niego, urządzeń zewnętrznych. 4. Funkcja blokowania/odblokowania gotowania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego stacji roboczej lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość – bez potrzeby uruchamiania systemu operacyjnego z dysku twardego stacji roboczej lub innych, podłączonych do niego urządzeń zewnętrznych – ustawienia hasła na poziomie administratora.
Bezpieczeństwo	BIOS musi posiadać możliwość: 1. Skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS. 2. Możliwość ustawienia hasła na dysku (drive lock). 3. Blokady/wyłączenia portów USB, COM, karty sieciowej. 4. Kontroli sekwencji boot-ującej. 5. Startu systemu z urządzenia USB. 6. Funkcja blokowania boot-owania stacji roboczej z zewnętrznych urządzeń. 7. Blokowania zapisu na dyskach wymiennych USB. Stacja robocza musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (min. TPM 2.0).
Klawiatura	1. Układ QWERTY. 2. Kolor czarny. 3. Interfejs: USB. 4. Blok numeryczny.

Specyfikacja Stacji Roboczej wraz z niezbędnym wyposażeniem – 2 szt.	
Mysz	Mysz przewodowa, optyczna, ze złączem USB, z min. dwoma przyciskami oraz rolką (scroll).

III.2.2 SPECYFIKACJA MONITORÓW.

Każdy dostarczony Monitor liczony jest jako zestaw, w skład którego wchodzi Monitor oraz niezbędne wyposażenie dodatkowe tj.:

Specyfikacja Monitora wraz z niezbędnym wyposażeniem dodatkowym – 4 szt.	
Produkt	Monitor
Wyposażenie dodatkowe	1. Monitor; 2. Podstawa Monitora. 3. Przewód zasilający. 4. Przewód DisplayPort męski-męski. 5. Przewód HDMI męski-męski.
Matryca	1. Matowa. 2. Podświetlenie matrycy LED. 3. Matryca obsługująca natywnie rozdzielczość 2560x1440. 4. Częstotliwość odświeżana min 144 Hz. 5. Przekątna min 27”. 6. Proporcje 16:9 lub 16:10. 7. Kąty widzenia: • Poziom: 178 stopni. • Pion: 178 stopni. 8. Jasność 350 cd/m2. 9. Kontrast 1000:1.
Interfejsy	1. Wejście HDMI min. 1.4 x 1. 2. Wejście DisplayPort min. 1.2 x1; 3. Wejście USB min. 2.0 typ A x2;
Funkcje ogólne	1. Technologia redukcji migotania; 2. Tryb ochrony oczu przed nadmiernym niebieskim światłem; 3. Język menu OSD polski lub angielski.
Cechy fizyczne	1. Regulacja wysokości w zakresie wysokości od min. 50 mm. do min. 130mm licząc odległość od dolnej krawędzi Monitora od powierzchni, na której stoi Monitor. 2. Obrotowy ekran (PIVOT) w zakresie min. 0-90 stopni. 3. Regulacja pochylenia (TILT) w zakresie min. -5-20 stopni. 4. Zgodny ze standardem VESA. 5. Kolor obudowy czarny, odcienie szarości lub srebrny. 6. Zasilacz wbudowany w bryłę Monitora.

Specyfikacja Monitora wraz z niezbędnym wyposażeniem dodatkowym – 4 szt.	
Zarządzanie energią	1. Pobór mocy podczas spoczynku (standby) max 0,5 W. 2. Klasa energetyczna min. B.

III.2.3 WYMAGANIA GWARANCYJNE DLA STACJI ROBOCZYCH I MONITORÓW

1.1. Przedmiotem zamówienia jest jednorazowa dostawa stacji roboczych i monitorów, zgodnie z specyfikacją wymienioną w OPZ i gwarancją producenta na okres minimum 36 miesięcy.

1.2. Dostarczony Sprzęt musi być objęty minimum 36 miesięczną gwarancją producenta, realizowaną w zakresie serwisu gwarancyjnego przez producenta lub autoryzowanego partnera serwisowego producenta.

1.3. Zasady świadczenia gwarancji dla Sprzętu:

1) Usunięcie awarii – do 14 Dni Roboczych od dnia zgłoszenia (przyjmowanie zgłoszeń w Dni Robocze przez 8h telefonicznie, faksem lub e-mailem),
2) Zamawiający zastrzega sobie prawo do samodzielnego demontażu/montażu dysku bez utraty gwarancji producenta;
3) w przypadku stwierdzenia uszkodzenia nośnika danych (np. dysku twardego HDD, dysku SSD), należy wymienić go na nowy, wolny od wad, o tych samych lub lepszych parametrach, bez zwrotu uszkodzonego dysku twardego HDD / SSD;