OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest:

- sprawowanie administracyjnej opieki nad należącymi do Zamawiającego: siecią IT, systemami informatycznymi, ich komponentami oraz urządzeniami wchodzącymi w ich skład, wraz z obsługą awarii i innych zgłoszeń od użytkowników oraz świadczeniem wsparcia merytorycznego i technicznego na ich rzecz;
- wsparcie dla Zamawiającego w zakresie cyberbezpieczeństwa oparte na całodobowym, codziennym monitoringu poziomu bezpieczeństwa.

I. DEFINICJE

Użyte w niniejszym OPZ wyrażenia mają następujące znaczenie:

1) **Cyberbezpieczeństwo** - odporność systemów informatycznych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
2) **Obsługa incydentu** - czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;
3) **Siła wyższa** - zdarzenie nadzwyczajne, zewnętrzne, którego nie można było przewidzieć i któremu nie można było zapobiec. Pojęcie siły wyższej nie obejmuje żadnych zdarzeń, które wynikają z niedołożenia przez wykonawcę należytej staranności w rozumieniu art. 355 § 2 kodeksu cywilnego;
4) **Operator usługi kluczowej** – podmiot, o którym mowa w załączniku nr 1 do ustawy z dnia 5 lipca 2018 r. O krajowym systemie cyberbezpieczeństwa (dz. U. 2018.1560 z dnia 13.08.2018), posiadający siedzibę na terytorium rzeczypospolitej polskiej, świadczący usługę kluczową, a której świadczenie zależy od systemów informacyjnych;
5) **System informatyczny** - system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity: dz.u.2023 poz. 57), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
6) **Usługa kluczowa** - usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych;
7) **Zagrożenie cyberbezpieczeństwa** - potencjalna przyczyna wystąpienia incydentu;
8) **Zarządzanie incydentem** - obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;

9) **Zarządzanie ryzykiem** - koordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka;
10) **Awaria** − zdarzenie, w którym uszkodzeniu uległ lub błędnie działa jeden (lub więcej) komponent systemu informatycznego, ograniczające wydajność lub funkcjonalność systemu informatycznego, utrudniające lub uniemożliwiające zamawiającemu lub partnerom korzystanie z systemu informatycznego zgodnie z jego przeznaczeniem;
11) **Awaria krytyczna** - awaria, która uniemożliwia Zamawiającemu lub partnerom świadczenie podstawowych usług;
12) **System biletowy** – system do obsługi zgłoszeń umożliwiający rejestracje, śledzenie, przekazywanie, kategoryzowanie, dostarczanie rozwiązań;
13) **Dzień** – dni kalendarzowe;
14) **Dzień roboczy** - dni tygodnia od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy;
15) **Kierownik Zamawiającego** – osoba lub organ, który – zgodnie z obowiązującymi przepisami, statutem lub umową – jest uprawniony do zarządzania zamawiającym;
16) **Obiekt** – budynki szpitala (główny i techniczny) zlokalizowane we Wrocławiu przy ul. Gen. Augusta Emila Fieldorfa 2 zarządzanego przez „Nowy Szpital Wojewódzki" sp. z o. o.;
17) **Użytkownik komputera, użytkownik systemu** (dalej: **Użytkownik**) – osoba korzystająca z systemu komputerowego; osoba, grupa osób, instytucja, organizacja lub nawet oddzielny system, który ma prawo do użytkowania systemu komputerowego;
18) **Użytkownik obiektu** – Dolnośląski Szpital Specjalistyczny im. T. Marciniaka – Centrum Medycyny Ratunkowej (z siedzibą: ul. Gen. Augusta Emila Fieldorfa 2, 54-049 Wrocław) wykorzystujący obiekt do prowadzenia działalności medycznej;
19) **Podmioty trzecie** – inne Firmy lub Osoby fizyczne (w tym producenci sprzętu lub oprogramowania), z którymi Zamawiający posiada zawarte bezpośrednie umowy, nie będące Stroną Umowy;
20) **Umowa** – niniejszy dokument wraz z załącznikami.

II. OPIS SZCZEGÓŁOWY OPIEKI ADMINISTRACYJNEJ NAD INFRASTRUKTURĄ IT:

1. Wykonawca zobowiązuje się do świadczenia opieki administracyjnej nad infrastrukturą IT Zamawiającego, zlokalizowaną w obiekcie szpitala przy ulicy Generała Fieldorfa 2 (54-049) we Wrocławiu oraz w biurze Zamawiającego przy ulicy Igielnej 13 (50-117) we Wrocławiu.

2. Usługi opieki w zakresie administracji infrastruktury IT obejmują:
    1) Administrowanie i utrzymanie sprawności infrastruktury IT Spółki składającej się w szczególności z:
        a) systemu wirtualizacji,
        b) serwerów aplikacyjnych,
        c) serwerów bazodanowych - zarządzanie systemami bazodanowymi w Podmiocie. Instalacja, administracja, optymalizacja wydajności, zarządzanie bazami danych (zasobami, kontami użytkowników, uprawnieniami), wykonywanie i regularne testowanie kopii zapasowych,
        d) systemu kopii zapasowych,
        e) systemów bezpieczeństwa (SIEM, SOAR, Firewalle, AV etc.),
        f) serwerów i macierzy,
        g) sieci LAN, WLAN , w tym:
            - ✓ 4 punkty styku WAN/LAN, w tym klaster UTM x 2 − w sumie 8 urządzeń UTM FortiGate.
            - ✓ 62 przełączniki sieciowe LAN HP-ARUBA/CISCO
            - ✓ AP: 224 sztuki
            - ✓ Wifi Kontroler x 4 sztuki
        h) monitoringu CCTV, systemu sygnalizacji włamań i napadu, systemu zarzadzania budynkiem, systemu kontroli do pomieszczeń,
        i) usługami AD, DNS, DHCP,
            i Infoblox – DNS, DHCP
            ii Windows Server - AD
        j) stacji roboczych – 34 sztuk
        k) drukarek sieciowych – 6 sztuki
    2) Administrowanie systemami chmurowymi spółki (poczta, dyski, komunikator).
    3) Bieżące wsparcie użytkowników oraz serwis komputerów, polegające na:
        a) pomocy użytkownikom w obsłudze komputerów oraz oprogramowania,
        b) rozwiązywaniu bieżących problemów z komputerami,
        c) instalacji dodatkowego sprzętu lub oprogramowania np.: komputera, drukarki, modemu etc.
        d) pomocy przy zmianach stanowiska pracy i przenosinach komputerów.
        e) usuwaniu awarii powstających w systemie informatycznym.
    4) Prowadzenie działań profilaktycznych wykonywanych raz na pół roku, polegających na przeglądzie konserwacyjnym serwerów (w ramach przeglądu: czyszczenie obudowy, czyszczenie wiatraków w zasilaczach etc.).
    5) Wykonywanie aktualizacji systemów operacyjnych komputerów oraz serwerów.

6) Rekomendowanie Zamawiającemu strategii rozwoju systemów IT spółki.
7) Sprawowanie nadzoru ogólnego nad realizacją inwestycji Zamawiającego (lub Użytkownika obiektu szpitalnego) w branży teletechnicznej, planowanie i koordynacja wdrożeń systemów IT w obszarach objętych przebudowami, remontami lub innymi działaniami mającymi wpływ na strukturę zasobów IT.
8) Przygotowanie opisów przedmiotu zamówienia do cyklicznych (prowadzonych co rok) postępowań o udzielenie zamówień publicznych na przedłużenie subskrypcji dla:
    - oprogramowania Tenable Nessus - Nessus Professional do monitorowania infrastruktury informatycznej;
    - oprogramowania Veeam Backup and Replication Standard;
    - systemu backupu Veeam Backup dla Microsoft 365;
    - macierzy i serwera Fujitsu;
    - 4 szt. HPE 5900AF-48XG-4QSFP+;
    - platformy wirtualizacji Vmware;
    - 2 szt. urządzeń FortiGate 500E;
    - urządzenia FortiGate 61E;
    - Fortianalyzer VM;
    - Microsoft 365 Business Standard.
9) Konsultacja merytoryczna przy przygotowywaniu i przeprowadzeniu przetargów w zakresie wyposażenia Zamawiającego oraz obiektu szpitala w systemy
10) i urządzenia z branży teletechnicznej.
11) Uczestnictwo w odbiorach systemów i urządzeń teletechnicznych.
12) Udział w pracach związanych z integracją systemów teleinformatycznych.
13) Współpraca z użytkownikiem obiektu szpitala oraz dzierżawcami w zakresie eksploatacji systemów i urządzeń teletechnicznych (w tym usuwanie i pomoc w usuwaniu awarii w części infrastruktury IT należącej do Zamawiającego).
14) Konfiguracja i diagnozowanie sieci i systemów teleinformatycznych oraz udział w projektowaniu nowych rozwiązań.
15) Administrowanie domeną(stroną) internetową.
16) Obsługa dostępów sieciowych oraz dostępów do danych dla pracowników Zamawiającego oraz innych osób przezeń wskazanych.
17) Obsługa dostępów do sieci Wi-Fi pacjentów i pracowników Szpitala im. T. Marciniaka.

3. Informacje o sprzęcie/systemach/urządzeniach:
    a. Serwerowe systemy operacyjne:
    - Windows Server 2016/2019/2022 – 12 sztuk,
    - Linux CentOS 7/8 – 8 sztuk,

- Linux Ubuntu 22 – 2 sztuki, Wirtualizacja:
- VMWare EsXI 7 + vCenter – 4 sztuki,

b. Centralny system kopii zapasowej:

- Backup: VeamBackup

c. Przełączniki sieciowe wymagające stałego nadzoru:

- 62 sztuki (urządzenia sieciowe typu HP 5500, HP 870, 1920) Firewalli brzegowych:
- 2 punkty styku WAN/LAN, w tym klaster UTM x 2, w sumie 3 urządzenia UTM FortiGate
- WiFi, AP: urządzenia marki HP
- 224 sztuki + kontroler,
- Macierz Fujitsu
- Eternus DX x 5 sztuk
- Ilość stacji roboczych, bezpośrednio w nadzorze serwisowym: 48 sztuk
- ilość serwerów, w tym serwery wirtualne: 24 sztuki
- Drukarki i inne urządzenia drukujące: 4 sztuki Dodatkowo:
- 1 kontroler wraz z 144 punktami systemu przyzywowego opartego o sieć LAN Usługi integracyjne wymagające stałego nadzoru:
- Microsoft Office 365/Microsoft Azure
- Microsoft AD kontroler domeny
- System kontroli dostępu
- System CCTV
- System kopii środowiska testowego VMWare

Uwaga: podane powyżej ilości jednostek sprzętu komputerowego, urządzeń sieciowych i innej aparatury objętej opieką administracyjną Wykonawcy, odnoszą się do stanu w dniu sporządzania niniejszego Opisu Przedmiotu Zamówienia. Wykonawca – bez roszczenia sobie prawa do zmian w wynagrodzeniu – musi założyć, że:

- **wraz z rozwojem firmy Zamawiającego oraz zmianą form jej działalności może nastąpić zwiększenie ilości stacji roboczych, licencji, drukarek i innych urządzeń końcowych i ich oprogramowania,**
- **wraz z rozbudową / modernizacją sieci Wi-Fi z pewnością nastąpi wzrost ilości urządzeń sieciowych, zmiana ich parametrów oraz charakterystyki.**

III. OPIS SZCZEGÓŁOWY OBOWIĄZKÓW WYKONAWCY ZWIĄZANYCH Z ZAPEWNIENIEM CYBERBEZPIECZEŃSTWA ZAMAWIAJĄCEGO:

1. Wykonawca zobowiązuje się do świadczenia usług wsparcia z zakresu cyberbezpieczeństwa dla Zamawiającego. Wsparcie w tym zakresie – oprócz czynności szczegółowo opisanych poniżej – obejmuje również bieżącą współpracę z Użytkownikiem obiektu szpitalnego przy ul. Generała Fieldorfa 2 we Wrocławiu, to jest Dolnośląskim Szpitalem Specjalistycznym im. T. Marciniaka – Centrum

Medycyny Ratunkowej. Podstawowym założeniem współpracy, o której mowa powyżej, jest fakt, że Użytkownik obiektu jest operatorem usługi kluczowej w rozumieniu obowiązujących przepisów i zapewnia sobie wymagany nimi poziom cyberbezpieczeństwa samodzielnie lub przez własne podmioty wykonawcze. Wykonawca usługi będącej przedmiotem niniejszego zamówienia będzie zobowiązany do takiego zakresu współpracy z osobami lub podmiotami wskazanymi przez Użytkownika obiektu, jaki umożliwi skuteczne prowadzenie przez ten podmiot czynności związanych z bieżącą kontrolą poziomu bezpieczeństwa cybernetycznego oraz skuteczną realizację przewidzianych prawem działań, jednak podmiotem każdorazowo odpowiedzialnym za te czynności i działania jest operator usługi kluczowej.

2. Niezależnie od powyższego Wykonawca odpowiedzialny jest za całodobowe, codzienne monitorowanie bezpieczeństwa teleinformatycznego Zamawiającego, w obu jego lokalizacjach, to jest:
   - lokalizacji biura spółki, mieszczącego się przy ul. Igielnej 13 (50-117) we Wrocławiu,
   - lokalizacji pionu eksploatacji, mieszczącego się w obiekcie szpitalnym przy ul. Generała Fieldorfa (54-049) we Wrocławiu.
3. Monitorowanie bezpieczeństwa teleinformatycznego, o którym mowa powyżej, obejmuje następujące czynności:
   - analiza bieżących polityk bezpieczeństwa i przedstawianie koordynatorom umowy z ramienia Zamawiającego propozycji ich zmian wraz z uzasadnieniem,
   - analizowania systemów informatycznych Zamawiającego pod względem ich odporności na zagrożenia cyberbezpieczeństwa i wprowadzenie niezbędnych zmian konfiguracyjnych, by zapewnić bezpieczeństwo teleinformatyczne i prawidłowo działanie systemów oraz współpracujących z nimi urządzeń,-
   - dostosowywanie systemów do aktualnych wymogów bezpieczeństwa dla:

     a. systemu wirtualizacji,
     b. systemu backupu,
     c. systemów bezpieczeństwa (SIEM, SOAR, Firewalle, UTM.),
     d. serwerów i macierzy,
     e. sieci LAN, WLAN oraz VoIP,
     f. stacji roboczych,
     g. drukarek sieciowych;

4. monitorowanie systemów chmurowych spółki Microsoft Exchange Office 365,
5. wykrywanie i obsługę incydentów przez 24 godziny na dobę, 7 dni w tygodniu przez 365 dni w roku,
6. zapewnienie dostępu do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT, NASK lub CSIRT GOV,
7. klasyfikację incydentów, wykrywanie podatności,

8. zgłoszenie lub rekomendowanie zgłaszania incydentów do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV,
9. zabezpieczanie informacji potrzebnych do analizy po włamaniowej na potrzeby postępowań prowadzonych przez organy ścigania,
10. analizę istniejących polityk bezpieczeństwa:

    1) zarządzanie incydentami;
    2) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa,
    3) wykrywanie i obsługę incydentów przez 24 godziny na dobę, 7 dni w tygodniu przez 365 dni w roku
    4) zapewnienie dostępu do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań;
    5) klasyfikację incydentu jako poważny na podstawie progów uznawania incydentu za poważny;
    6) zgłoszenie incydentów do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
    7) współdziałanie podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV;
    8) badanie odporności systemów informatycznych na przełamanie lub omijanie zabezpieczeń za pomocą skanerów podatności zaktualizowanych o bazy CVE;
    9) analizowanie kodu oprogramowania szkodliwego i określanie jego wpływu na system klienta;
    10) zabezpieczanie informacji potrzebnych do analizy powłamaniowej na potrzeby postępowań prowadzonych przez organy ścigania;
    11) sporządzanie miesięcznych raportów z działalności komórki - zawierających zestawienie incydentów wraz z opisem i dalszymi zaleceniami.
    12) analizę istniejących polityk bezpieczeństwa;
    13) zarządzanie dokumentacją cyberbezpieczeństwa;
    14) zarządzanie ryzykiem;

11. Wykonawca zapewnia wykonanie Przedmiotu umowy przez osoby posiadające odpowiednie doświadczenie i kwalifikacje.

Wykonawca winien spełniać warunki udziału w postępowaniu w zakresie zdolności technicznej lub zawodowej, jeśli wykaże, że:

1) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał lub wykonuje w przypadku świadczeń powtarzających się lub ciągłych, nieprzerwanie przez okres co najmniej 6 miesięcy, co najmniej 2 (dwie) usługi polegające na wsparciu i administrowaniu systemem teleinformatycznym, obejmującym co najmniej 100 jednocześnie zalogowanych użytkowników.

2) dysponuje osobami - posiadającymi:

a) w zakresie cyberbezpieczeństwa (co najmniej 1 osoba) – wiedzę i umiejętności w zakresie analizy zagrożeń, reagowania na zagrożenia i incydenty, identyfikacji złośliwej aktywności.

b) w zakresie opieki administracyjnej nad infrastrukturą IT (co najmniej 2 osoby) - znajomość poniższych zagadnień:

- administrowanie serwerami Microsoft,
- administrowanie urządzeniami sieciowymi z ważnym certyfikatem producenta urządzeń posiadanych przez Zamawiającego,
- utrzymanie i zarządzanie urządzeniami typu Firewall na poziomie eksperckim z ważnym certyfikatem producenta urządzeń posiadanych przez Zamawiającego.

W przypadku skierowania przez Wykonawcę do sprawowania opieki administracyjnej nad infrastrukturą IT więcej niż 1 osoby, osoby te mogą spełniać powyższy warunek łącznie;

c) wykształcenie wyższe (min. licencjat lub inżynier) oraz co najmniej 2 letnie doświadczenie w zakresie wsparcia IT.

12. Zamawiający zobowiązuje się ponadto do przekazania Wykonawcy dokumentacji posiadanych systemów informatycznych w zakresie niezbędnym do realizacji zamówienia.

13. Wykonawca zobowiązuje się do udostępnienia Zamawiającemu systemu biletowego. Zamawiający będzie wykonywał zgłoszenia serwisowe poprzez wysyłanie wiadomości email na wskazany przez Wykonawcę adres poczty elektronicznej. System biletowy automatycznie powiadomi użytkownika o statusie realizacji zgłoszenia. Zamawiający po podpisaniu umowy przekaże listę osób, które będą mogły wykonywać zgłoszenia w systemie biletowym. Dodatkowo Wykonawca zapewni dostęp poprzez stronę www Zamawiającemu do zgłoszeń wykonanych przez pracowników NSzW.

14. W przypadku awarii krytycznej Zamawiający wykona zgłoszenie w systemie biletowym, a następnie wykona połączenie telefoniczne w celu weryfikacji przyjęcia zgłoszenia. W przypadku braku możliwości wykonania zgłoszenia w systemie biletowym, Wykonawca zobowiązany jest przyjąć zgłoszenie telefonicznie. W takich sytuacjach za godzinę przyjęcia zgłoszenia przez Wykonawcę uznaje się godzinę skutecznego połączenia telefonicznego i przekazania informacji o awarii krytycznej. Na Wykonawcy ciąży obowiązek udokumentowania zarówno czasu przyjęcia zgłoszenia, jak też czasu reakcji i rozwiązania problemu związanego ze zgłoszeniem.

15. Wykonawca zobowiązuje się do oddelegowania pracownika aby był obecny w obiekcie szpitala przy ulicy Generała Fieldorfa 2 przez cały czas obowiązywania umowy, w dni powszednie od godziny **Od 09:00 do 13:00** Wyjątkiem od powyższego wymogu są sytuacje świadczenia opieki w biurze Zamawiającego, w terminach wcześniej uzgodnionych z Zamawiającym.

16. Wykonawca zobowiązuje się do umożliwienia kontaktu telefonicznego z personelem oddelegowanym do **realizacji przedmiotu umowy poza godzinami świadczenia usługi, to jest w godzinach od 13:00 do 09:00** w dni powszednie oraz całodobowo w dni wolne od pracy. Kontakt ten będzie wykorzystywany wyłącznie w sytuacjach awarii krytycznej, niosących z sobą istotne zagrożenie dla funkcjonowania zlokalizowanej w obiekcie placówki medycznej.

17. Zamawiający wymaga, by reakcją Wykonawcy na zgłoszenie awarii krytycznej było niezwłoczne (**nie późniejsze niż w okresie 30 minut od zgłoszenia**) podjęcie działań zmierzających do usunięcia zgłoszonej awarii, poprzez zdalne przywrócenie prawidłowego funkcjonowania objętej awarią części infrastruktury, lub przyjazd do obiektu szpitalnego przy ul. Gen. Fieldorfa 2 we Wrocławiu i usunięcie awarii.

18. W celu realizacji zamówienia Zamawiający, niezwłocznie po podpisaniu umowy, nie później niż w ciągu **14 dni** - udzieli Wykonawcy informacji o użytkowanych systemach oraz dostarczy logi z:
    1) posiadanych systemów bezpieczeństwa, w tym m.in. systemów AV, Firewall,
    2) urządzeń sieciowych,
    3) kontrolera domeny,
    4) systemów bazodanowych,
    5) systemów DHCP, DNS,
    6) innych systemów mogących mieć wpływ na świadczenie usługi kluczowej.

19. Zamawiający zobowiązuje się ponadto do przekazania Wykonawcy dokumentacji posiadanych systemów informatycznych w zakresie niezbędnym do realizacji zamówienia.
20. Wykonawca zobowiązany jest do prowadzenia wszelkich prac tak aby nie kolidowały z działalnością leczniczą jednostki, z poszanowaniem dobra pacjentów. Informacje o planowanych włączeniach/wyłączeniach urządzeń Wykonawca będzie przekazywał Zamawiającemu z wyprzedzeniem – co najmniej 1 Dzień roboczy. W przypadku braku możliwości podjęcia czynności usuwania awarii w czasie dłuższym niż 30 min. z przyczyn niezależnych od Wykonawcy, Wykonawca zobowiązany jest udzielić Zamawiającemu informacji zwrotnej z przewidywalnym czasem usunięcia awarii oraz jej przyczyną.
21. Wykonawca zobowiązany jest do przekazywania raportu za poprzedni miesiąc z wykonywanych czynności oraz obsłużonych zgłoszeń w systemie biletowym.

Wzór raportu tygodniowego/miesięcznego

Data	Zadanie/zdarzenie	Przyczyna, podjęte działania i rezultat