WSTĘPNY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem niniejszego zamówienia są usługi z zakresu:

a) cyberbezpieczeństwa,
b) opieki administracyjnej nad systemem informatycznym oraz jego komponentami i urządzeniami wchodzącymi w jego skład, wraz z obsługą awarii i innych zgłoszeń od użytkowników oraz świadczeniem wsparcia merytorycznego i technicznego na ich rzecz.

I. DEFINICJE

Użyte w niniejszym OPZ wyrażenia mają następujące znaczenie:

1) CSIRT GOV - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
2) CSIRT MON - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;
3) CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy;
4) cyberbezpieczeństwo - odporność systemów informatycznych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
5) incydent - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
6) incydent krytyczny - incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;
7) incydent poważny - incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;
8) komórka SOC – wyspecjalizowana pod względem osobowym i technicznym jednostka Wykonawcy świadcząca usługi z zakresu cyberbezpieczeństwa;
9) obsługa incydentu - czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;
10) 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;
11) 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;
12) 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;

13) usługa kluczowa - usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych;
14) zagrożenie cyberbezpieczeństwa - potencjalna przyczyna wystąpienia incydentu;
15) zarządzanie incydentem - obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;
16) zarządzanie ryzykiem - koordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka;
17) 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;
18) awaria krytyczna - awaria, która uniemożliwia Zamawiającemu lub Partnerom świadczenie Podstawowych Usług;
19) system biletowy – system do obsługi zgłoszeń umożliwiający rejestracje, śledzenie, przekazywanie, kategoryzowanie, dostarczanie rozwiązań;

II. OPIS SZCZEGÓŁOWY SOC:

1. Wykonawca zobowiązuje się do świadczenia usług wsparcia z zakresu cyberbezpieczeństwa dla operatorów usług kluczowych obsługiwanych przez Zamawiającego, w chwili obecnej jest to 2 operatorów (szpitale).
2. Zamówienie będzie realizowane w lokalizacji: obiekt szpitala przy ul. Fieldorfa 2 we Wrocławiu w pomieszczeniach udostępnionych przez Zamawiającego.
   Zamawiający dysponuje pomieszczeniem służącym do świadczenia usług stanowiących przedmiot niniejszej zamówienia, które zabezpieczone jest przed zagrożeniami fizycznymi oraz środowiskowymi, a także stosuje odpowiednie zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji.
3. Usługi wsparcia w zakresie cyberbezpieczeństwa obejmują:
   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) sporządzanie corocznej analizy ryzyka w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji;
13) analizę istniejących polityk bezpieczeństwa;
14) zarządzanie dokumentacją cyberbezpieczeństwa;
15) zarządzanie ryzykiem;
16) audyty bezpieczeństwa [Wykonawca zleci firmie zewnętrznej wykonanie dwóch audytów bezpieczeństwa systemu informacyjnego zgodnie z wymaganiami obowiązujących przepisów. Pierwszy audyt musi zostać wykonany w grudniu 2024, a następny po dwóch latach. Firma audytująca musi dysponować osobą posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu Dz.U. z 2018 r. poz. 1999].

4. Wykonawca zapewnia wykonanie Przedmiotu umowy przez osoby posiadające odpowiednie doświadczenie i kwalifikacje.
5. W ramach zadań wykonywanych przez komórkę „SOC" Wykonawca ma obowiązek:
    1) identyfikowania zagrożenia w odniesieniu do systemów informacyjnych operatora usługi kluczowej,
    2) proponowania rozwiązania ograniczającego ryzyko wynikające z zagrożenia systemów informacyjnych,
    3) analizowania oprogramowania szkodliwego i określenia wpływu tego oprogramowania na system informacyjny operatora usługi kluczowej;
    4) wykrywania przełamywania lub omijania zabezpieczeń systemu informacyjnego operatora usługi kluczowej,
    5) prowadzenia analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego,
    6) zabezpieczenia informacji potrzebnych do analizy powłamaniowej na potrzeby ewentualnego postępowania sądowego.
6. W przypadku wystąpienia incydentu, Wykonawca zobowiązany jest do jego zgłoszenia niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym (CSIRT), a prowadzonym przez właściwy organ.
7. Zgłoszenie, o którym mowa wyżej, przekazywane jest w postaci elektronicznej lub przy użyciu innych dostępnych środków komunikacji i zawiera:
    1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres;
    2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;
    3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;

4) opis wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym:
   a) usługi kluczowe zgłaszającego, na które incydent poważny miał wpływ,
   b) liczbę użytkowników usługi kluczowej, na których incydent poważny miał wpływ,
   c) moment wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania,
   d) zasięg geograficzny obszaru, którego dotyczy incydent poważny,
   e) wpływ incydentu poważnego na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych,
   f) przyczynę zaistnienia incydentu poważnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe;
5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie, czy incydent dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej;

8. Wykonawca zobowiązany jest, na żądanie Zamawiającego, do przekazywania do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym (CSIRT) informacji o innych niż poważne incydentach, o zagrożeniach cyberbezpieczeństwa, dotyczących szacowania ryzyka, o podatnościach i o wykorzystywanych technologiach.
9. Informacje, o których mowa w ust. 8 przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.
10. Współdziałając przy obsłudze incydentu poważnego i krytycznego, Wykonawca zobowiązany jest do przekazywania Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym (CSIRT) niezbędnych danych, w tym danych osobowych.
11. Wykonawca zobowiązuje się do oznaczania przekazywanych informacji jako informacji stanowiących tajemnice prawnie chronione pod warunkiem ich wyraźnego uznania za stanowiące tajemnice prawnie chronione przez Zamawiającego.
12. Wykonawca zobowiązany jest do informowania Zamawiającego o wszelkich istotnych okolicznościach mających wpływ na należyte wykonywanie umowy, w tym w szczególności o przeszkodach i utrudnieniach związanych z realizacją usług.
13. W celu realizacji zamówienia Zamawiający, nie zwłocznie po podpisaniu umowy, nie później niż w terminie 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.
14. Zamawiający zobowiązuje się ponadto do przekazania Wykonawcy dokumentacji posiadanych systemów informatycznych w zakresie niezbędnym do realizacji zamówienia.

III. 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
      h) monitoringu CCTV, systemu sygnalizacji włamań i napadu, systemu zarzadzania budynkiem, systemu kontroli do pomieszczeń,
      i) usługami AD, DNS, DHCP,
      j) stacji roboczych,
      k) drukarek sieciowych.
   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) Konsultacja merytoryczna przy przygotowywaniu i przeprowadzeniu przetargów w zakresie wyposażenia Zamawiającego oraz obiektu szpitala w systemy i urządzenia z branży teletechnicznej.
   9) Uczestnictwo w odbiorach systemów i urządzeń teletechnicznych.
   10) Udział w pracach związanych z integracją systemów teleinformatycznych.
   11) 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).

12) Konfiguracja i diagnozowanie sieci i systemów teleinformatycznych oraz udział w projektowaniu nowych rozwiązań.
13) Administrowanie domeną(stroną) internetową. (Czy wykonawca będzie musiał wykonywać publikacje i czy będzie odpowiadał ze jej zabezpieczenie.)
14) Obsługa dostępów sieciowych oraz dostępów do danych dla pracowników Zamawiającego oraz innych osób przezeń wskazanych.
15) Obsługa dostępów do sieci Wi-Fi pacjentów i pracowników Szpitala im. T. Marciniaka.

3. Wykonawca zobowiązuje się do udostępnienia Zamawiającemu systemu biletowego. Zamawiający będzie wykonywał zgłoszenia serwisowe poprzez wysyłanie wiadomości e-mail 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.
4. 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.
5. 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 08:00 do godz.16:00. Wyjątkiem od powyższego wymogu są sytuacje świadczenia opieki w biurze Zamawiającego, w terminach wcześniej uzgodnionych z Zamawiającym.
6. Wykonawca zobowiązuje się do umożliwienia kontaktu telefonicznego z personelem oddelegowanym do realizacji przedmiotu umowy poza godzinami świadczenia usługi, to jest w godzinach od 16:00 do 08:00 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.
7. 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.
8. W celu realizacji zamówienia Zamawiający, niezwłocznie po podpisaniu umowy - 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.

9. Zamawiający zobowiązuje się ponadto do przekazania Wykonawcy dokumentacji posiadanych systemów informatycznych w zakresie niezbędnym do realizacji zamówienia.
10. 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. 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.
11. 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