OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

na świadczenie usług utrzymania, administracji i rozwoju infrastruktury oraz systemów teleinformatycznych Zamawiającego

1. Przedmiot zamówienia

Przedmiotem zamówienia jest świadczenie usług obejmujących administrację, utrzymanie, rozwój oraz wsparcie użytkowników infrastruktury i systemów teleinformatycznych eksploatowanych przez Zamawiającego, tak aby zapewnić:

- ciągłość działania systemów,
- bezpieczeństwo informacji i ochronę danych osobowych,
- zgodność z przepisami prawa i regulacjami wewnętrznymi,
- możliwość odtworzenia środowiska po awarii, zdarzeniu lub incydencie
- bieżące całodobowe wsparcie dla użytkowników we wszystkich kwestiach związanych z funkcjonowaniem systemów/programów/ aplikacji występujących u Zamawiającego
- pełnienie roli Administratora Systemu Informatycznego
- szkolenia grupowe i indywidualne.

Zamawiający korzysta z następujących systemów, oprogramowania i technologii oraz wymaga znajomości w poniższych obszarach:

- produkty Microsoft: SQL Server, Windows Server, SharePoint, WSUS, AD DS, DHCP, DNS, IIS, Hyper-V,
- systemy IBM iSeries, Assure Mimix, BMS,
- systemy bezpieczeństwa UTM WatchGuard (konfiguracja HA i VPN),
- oprogramowanie: Axence nVision, Cognos Analytics, enova365, Bank Krwi, KRDK oraz e-Krew, e-Hemofilia – w trakcie wdrażania,
- procesy walidacji systemów skomputeryzowanych,
- administrację środowiskiem sieciowym (VLAN, VPN, segmentacja, DNS),
- zarządzanie kopiami zapasowymi i politykami bezpieczeństwa informacji.

Słownik pojęć:

Active Directory (AD) – usługa katalogowa firmy Microsoft przeznaczona do centralnego zarządzania użytkownikami, komputerami, grupami oraz uprawnieniami w domenie organizacji.

Administracja – zespół czynności konfiguracyjnych i nadzorczych wykonywanych na systemach i usługach, obejmujący m.in. zakładanie kont, nadawanie uprawnień, zmianę konfiguracji oraz kontrolę poprawności działania usług.

Awaria krytyczna – zdarzenie powodujące całkowity brak działania systemu Bank Krwi, e-Krew, środowiska serwerowego, systemów bazodanowych, jak również brak dostępu do infrastruktury sieciowej, brak możliwości realizacji statutowej działalności Zamawiającego.

Awaria – zdarzenie powodujące ograniczenie funkcjonalności elementów środowiska IT bez całkowitego wstrzymania pracy lub inny błąd w działaniu środowiska IT niepowodujący istotnego zakłócenia Ciągłości działania.

BI (Business Intelligence) – oprogramowanie i mechanizmy raportowo-analityczne umożliwiające przygotowywanie zestawień i analiz na podstawie danych pochodzących z systemów źródłowych Zamawiającego.

Ciągłość działania – zdolność środowiska IT do nieprzerwanego świadczenia usług na poziomie wymaganym przez Zamawiającego, pomimo występowania awarii.

Czas reakcji – maksymalny czas od zgłoszenia przez Zamawiającego do podjęcia działań (rozumiane jako rozpoczęcie faktycznej diagnozy problemu oraz kontakt z Zamawiającym) przez Wykonawcę.

Czas usunięcia awarii lub Awarii krytycznej – maksymalny czas przewidziany na przywró cenie poprawnego działania elementu środowiska IT, rozumianego jako przywrócenie pełnej funkcjonalności tego elementu lub zapewnienie rozwiązania zastępczego umożliwiającego realizację procesów Zamawiającego

DNS (Domain Name System) – usługa sieciowa odpowiedzialna za tłumaczenie nazw domenowych na adresy IP, niezbędna do prawidłowego działania usług w infrastrukturze Zamawiającego.

IOD (Inspektor Ochrony Danych) – osoba wyznaczona przez Zamawiającego do nadzoru nad zgodnością przetwarzania danych osobowych z przepisami prawa oraz wewnętrznymi regulacjami w tym zakresie.

Infrastruktura teleinformatyczna – całość zasobów sprzętowych i programowych Zamawiającego, obejmująca w szczególności serwery, macierze, sieć LAN/WAN, stacje robocze, urządzenia peryferyjne, systemy bezpieczeństwa oraz systemy specjalistyczne.

Microsoft SQL Server – system zarządzania relacyjną bazą danych firmy Microsoft wykorzystywany przez Zamawiającego jako platforma dla systemów i aplikacji.

Odtworzenie środowiska po awarii – proces przywrócenia działania do stanu sprzed awarii z wykorzystaniem kopii zapasowych oraz obowiązujących procedur (DR – Disaster Recovery).

PBI – Polityka bezpieczeństwa / polityka kopii zapasowych – zbiór obowiązujących u Zamawiającego zasad i procedur określających sposób zabezpieczania informacji, ochrony danych oraz wykonywania i przechowywania kopii zapasowych.

Raport SLA (Service Level Agreement) – dokument podsumowujący jakość i dostępność świadczonych usług IT w określonym czasie (miesiąc), potwierdzający zgodność z umową. Zawiera kluczowe metryki takie jak procent dostępności usług (uptime), czas reakcji i rozwiązania incydentów oraz status działań naprawczych.

Kluczowe elementy raportu SLA:

- Incydenty i awarie zgłaszane w dni robocze po godzinie 15:05 oraz w soboty i dni ustawowo wolne od pracy: liczba zgłoszeń, ich priorytet oraz czas potrzebny na ich usunięcie.

Rozwój systemów – prace polegające na rozbudowie, dostosowaniu lub optymalizacji funkcjonalności istniejących systemów w celu spełnienia aktualnych potrzeb Zamawiającego (np. wdrożenie nowych modułów, integracji, raportów).

System – system użytkowany przez Zamawiającego.

System kluczowy - System Bank Krwi oraz każdy inny system wskazany przez Zamawiającego jako krytyczny.

Segmentacja sieci – podział sieci teleinformatycznej na odrębne logiczne segmenty (np. VLAN) w celu zwiększenia bezpieczeństwa, kontroli ruchu oraz ograniczenia skutków ewentualnych incydentów.

System ERP – system do obsługi procesów finansowo-księgowych, kadrowych i organizacyjnych, magazynowych, dostępny przez przeglądarkę.

System e-Krew – to ogólnopolski, informatyczny system cyfryzacji publicznej służby krwi. Umożliwia krwiodawcom rezerwację wizyt, dostęp do wyników badań i zaświadczeń online, a centrom krwiodawstwa – obsługę całego procesu obsługi i kwalifikacji dawcy, poboru krwi, produkcji, ekspedycji i zarządzania stanami składników krwi oraz moduł BI do analizy i statystyki danych.

System e-Hemofilia – system informatyczny gromadzący dane pacjentów chorych na hemofilię i pokrewne skazy krwotoczne, który utworzy rejestr pacjentów, udostępni indywidualne karty postępowania oraz dzienniczki pacjenta przez Internetowe Konto Pacjenta. Umożliwi śledzenie, monitorowanie leczenia i prowadzenie leczenia lekami z NPLH.

System Bank Krwi – system informatyczny firmy Asseco, na którym pracują jednostki organizacyjne publicznej służby krwi w celu rejestracji dawcy krwi, pobrania krwi i jej składników, przetworzenia, zbadania i dopuszczenia do zastosowania klinicznego oraz wydania do podmiotów leczniczych krwi i jej składników. Prowadzi rejestr dawców i biorców krwi

System EZD RP (Elektroniczne Zarządzanie Dokumentacją) – bezpłatny, nowoczesny system informatyczny tworzony przez Ministerstwo Cyfryzacji i NASK, służący do obsługi korespondencji i dokumentów w administracji publicznej.

System monitoringu / NMS (Network Management System) – system klasy nadzorczo-monitorującej służący do bieżącego monitorowania infrastruktury, generowania alarmów oraz sporządzania raportów dotyczących jej pracy.

System serwerowy Microsoft Windows Server – system operacyjny firmy Microsoft przeznaczony do świadczenia usług serwerowych i uruchamiania usług infrastrukturalnych w środowisku Zamawiającego.

Środowisko IT - zbiór wzajemnie powiązanych zasobów sprzętowych (Infrastruktura informatyczna), programowych (Systemy) oraz sieciowych, któ re wspólnie umożliwiają

działanie Systemów w organizacji Zamawiającego, w tym zasoby zlokalizowane w siedzibie głównej oraz terenowych oddziałach Zamawiającego.

Utrzymanie (eksploatacja) – bieżące działania operacyjne zapewniające poprawną i ciągłą pracę systemów informatycznych, obejmujące m.in. monitoring, instalację aktualizacji, reagowanie na awarie, wykonywanie kopii zapasowych oraz działania prewencyjne zapobiegające występowaniu awarii

UTM (Unified Threat Management) – urządzenie klasy firewall integrujące wiele mechanizmów bezpieczeństwa (m.in. filtrację ruchu, VPN, IPS, antywirus), stosowane do ochrony sieci Zamawiającego.

VPN (Virtual Private Network) – bezpieczny, szyfrowany kanał komunikacyjny umożliwiający użytkownikom zdalny dostęp do zasobów wewnętrznych Zamawiającego.

Wsparcie użytkowników (service desk) – usługa polegająca na udzielaniu pomocy użytkownikom końcowym Zamawiającego w zakresie obsługi systemów, diagnozowania i usuwania zgłoszonych problemów oraz przekazywania ich do dalszej obsługi.

Zgłoszenie– informacja od użytkownika lub z systemu o nieprawidłowym działaniu wymagającym reakcji Wykonawcy. Zgłoszenie uznaje się za przyjęte w momencie jego rejestracji lub potwierdzenia przyjęcia przez Wykonawcę.

Posiadane zasoby:

liczba używanych PC	RCKiK - 146 szt. (Kraków - zestawy stacjonarne+laptopy) TO - 128 szt. (zestawy stacjonarne+laptopy)
liczba i rodzaj urządzeń sieciowych	RCKiK: Rozdzielacz sieciowy Avaya 220-24P-10GE2 – 2 szt. Rozdzielacz sieciowy 380-24T – 1 szt. Router HPE seria MSR 3000 – 3 szt. Router HPE seria MS930 – 1 szt. Przełącznik sieciowy Switch Nortel 4548GT – 3 szt. Przełącznik sieciowy Switch ERS 24 – 1 szt. Przełącznik sieciowy Ethernet ERS Seria 5000 – 2 szt. Przełącznik sieciowy Avaya 220-24P-10GE2 – 2 szt. Przełącznik Extreme Networks Avaya ERS 5952GTS – 2 szt. Przełącznik Avaya 220-24P-10GE2 – 1 szt. Urządzenie sieciowe Nortel Switch 5520/24 – 1 szt. Urządzenie dostępowe Eyherwerx – 1 szt. Urządzenie dostępowe do sieci Router Typ 1 – 1 szt.

	TO: Router HPE seria MSR930 Urządzenie dostępowe do sieci Router Typ 1 Urządzenie dostępowe do sieci Router 50000 LAN, Router HPE seria MSR930 -9 szt. Switch HPE CX 6000 48G (R8N85A) – 7 szt.
liczba i rodzaj sieci WiFi	jeden punk dostępowy dla Działu dawców
model routera brzegowego	UTM WatchGuard M360 FireCluster HP MSR3xxx series - 2 sztuki
liczba serwerów fizycznych (model) i liczba VM jakie się na nich znajdują	Serwer Primergy RX1330 M4/REACT Serwer IBM wraz z oprogramowaniem/REACT Serwer TX1310 M1 E3-1246v3 – 2 szt. Serwer IBM Power 8 Serwer Fujitsu Siemens Primergy RX300 S4 Serwer DELL R730 Serwer Cognos z oprogramowaniem // 9 maszyn wirtualnych HyperV
model kontrolera sieci	Microsoft AD (Active Directory z usługami wyszczególnionymi w opisie systemów)
liczbę i ilość NAS	macierz Infotrend
aplikacje do zarządzania	Axence nVision, Microsoft DC
poczta	usługa zewnętrzna
aplikacje MS365	MS365 z aplikacjami towarzyszącymi: OneDrive, MSTeams

Część urządzeń działa też na GSM.

2. Zakres przedmiotu zamówienia

2.1. Serwery, systemy serwerowe i systemy bazodanowe

a. Administracja i utrzymanie serwerów w środowisku Zamawiającego - środowisko serwerowe oparte na systemach Microsoft Windows Server w wersji 2012 lub nowszych.
b. Pełna administracja usługą Active Directory, obejmująca m.in.: zarządzanie grupami i kontami użytkowników, obiektami komputerów oraz jednostkami organizacyjnymi (OU), dostosowanie struktury katalogu do struktury organizacyjnej Zamawiającego oraz konfiguracja i utrzymanie zasad grup (GPO).
c. Obsługa serwerów kopii zapasowych planowanie i realizacja w testach odtworzeniowych.

d. Wykonywanie czynności administracyjnych w środowisku IBM iSeries/Power, reagowanie na występujące błędy oraz współpraca z podmiotami powiązanymi z Zamawiającym w zakresie diagnostyki, analizy i optymalizacji pracy serwerów.
e. Administracja Microsoft SQL Server: instalacja, konfiguracja, optymalizacja, uprawnienia oraz wykonywanie kopii bezpieczeństwa . Zamawiający korzysta aktualnie ze serwerów MS SQL w wersji 2008 lub nowszych.
f. Nadzór nad prawidłowością integracji przepływu danych pomiędzy systemami użytkowanymi przez Zamawiającego,
g. Nadzór nad środowiskiem wirtualnym i maszynami w infrastrukturze Zamawiającego – Microsoft HyperV.
h. Konfiguracja i nadzór nad lokalną usługą DNS.
i. Archiwizacja baz danych, dokumentowanie wykonywania kopii oraz przeprowadzanie testów odtworzeniowych zgodnie z przyjętą przez Zamawiającego polityką bezpieczeństwa i polityką wykonywania kopii zapasowych w formie papierowej lub elektronicznej
j. Administracja serwerem poczty oraz hostingiem Zamawiającego a w szczególności:
    - Konfiguracja usług,
    - Wykonywanie cyklicznych kopii zapasowych,
    - Konsultacje techniczne,
    - Administracja skrzynkami pocztowymi,
    - Administracja strefami DNS,
    - Zarządzanie domeną oraz subdomenami w imieniu Zamawiającego,
    - Serwer FTP – zarządzanie uprawnieniami.

2.2. Bezpieczeństwo i monitoring

a. Administracja oprogramowaniem antywirusowym posiadanym przez Zamawiającego, w tym tworzenie polityk, aktualizacje oraz monitoring stacji końcowych.

b. Współpraca z Inspektorem Ochrony Danych w zakresie tworzenia bezpiecznej polityki przetwarzania danych i procedur działania w zakresie bezpieczeństwa danych i cyberbezpieczeństwa
c. Administracja systemem monitoringu/nadzoru klasy NMS lub równoważnym – konfiguracja, alarmy, raportowanie.

2.3. Sieć LAN i WAN

a. Administracja siecią Zamawiającego, urządzeniami brzegowymi i urządzeniami klasy UTM – konfiguracja, monitoring, proaktywne reagowanie na zagrożenia, okresowa analiza logów na urządzaniu brzegowym, wdrażanie polityk bezpieczeństwa zgodnie z przyjęta przez Zamawiającego PBI oraz dobrymi praktykami. Zamawiający oświadcza, że aktualnie używa urządzeń klasy UTM WatchGuard w konfiguracji wysokiej dostępności.
b. Przeprowadzanie konfiguracji sieci w zakresie niezbędnej segmentacji, kontroli dostępu oraz monitorowania i konfiguracji VPN, zgodnie z dobrymi praktykami bezpieczeństwa transmisji danych oraz PBI.
c. Usuwanie awarii sieciowych.

2.4. Stacje robocze, serwery i urządzenia peryferyjne

a. Serwisowanie i konserwacja stacji roboczych i serwerów (z wykluczeniem urządzeń pozostających w okresie gwarancyjnym).
b. Przeglądy i konserwacja urządzeń peryferyjnych (drukarki, skanery) – z wykluczeniem sprzętu objętego gwarancją.
c. Przygotowanie lub odtwarzanie stanowisk roboczych (w tym instalacja niezbędnego na danym stanowisku oprogramowania i sterowników).
d. Usuwanie bieżących usterek w sprzęcie komputerowym - z wyłączeniem części zamiennych oraz urządzeń objętych gwarancją lub na aktualnych umowach serwisowych
e. Dokonywanie co najmniej raz do roku przeglądu stacji roboczych, urządzeń peryferyjnych oraz serwerów zainstalowanych w placówkach zarządzanych przez Zamawiającego – z wyłączeniem serwerów i zasilaczy awaryjnych objętych aktywną gwarancją. Wykonawca

zobowiązuje się do wykonywania przeglądów na własny koszt i we własnym zakresie korzystając z własnych materiałów,

Przez materiały, rozumie się materiały eksploatacyjne niezbędne do konserwacji (np. sprężone powietrze, środki czystości, smary). Wszelkie części zamienne (np. dyski twarde, pamięci RAM, zasilacze, tonery, części do drukarek) dostarcza Zamawiający lub są one przedmiotem osobnej wyceny i akceptacji.

2.5. Obsługa specyficznych systemów używanych przez Zamawiającego

Wykonawca obejmuje administracją, utrzymaniem i wsparciem konkretnie wskazane systemy używane przez Zamawiającego, w szczególności:

a. **System „Bank Krwi" (firmy Asseco**) **system informatyczny obsługujący jednostki organizacyjne publicznej służby krwi** – znajomość funkcjonalna i merytoryczna modułów: rejestracja, dział pobrań, pracownia analityczna, serologia, serodiagnostyka, preparatyka, ekspedycja, dział zapewnienia jakości, HLA, a także obsługa słowników oraz modułu Administrator zapewniająca wsparcie użytkowników Zamawiającego w zakresie obsługi i rozwoju oprogramowania. Umiejętność tworzenia oraz obsługi zapytań SQL w celu przygotowywania zestawień na żądanie Zamawiającego. Obsługa systemu zgłoszeń (JIRA) wykorzystywanego przez producenta oprogramowania oraz współpraca z dostawcą w zakresie zgłaszania błędów, inicjowania rozwoju aplikacji oraz usuwania usterek w oprogramowaniu. Instalacja i podstawowa konfiguracja oprogramowania do transmisji danych z aparatów medycznych i urządzeń użytkowanych przez Zamawiającego.

b. **System „e-Krew" (Centrum e-Zdrowia)** – udział w procesie wdrażania oprogramowania, konsultacje techniczne oraz merytoryczne z Zamawiającym, wsparcie Zamawiającego przy procesie migracji danych. Administracja użytkownikami oraz konfiguracją systemu w sytuacji przyznania uprawnień.

c. **System „e-Hemofilia"** – udział w procesie wdrażania oprogramowania, konsultacje techniczne oraz merytoryczne z Zamawiającym, wsparcie Zamawiającego przy procesie migracji danych. Administracja użytkownikami oraz konfiguracją systemu w sytuacji przyznania uprawnień.

d. **Oprogramowanie klasy ERP - „enova365 WEB" (Soneta)** – zarządzanie użytkownikami, słownikami, konfiguracją oprogramowania, w tym współpraca z dostawcą oprogramowania w zakresie zgłaszania błędów, rozwoju i usuwania błędów w oprogramowaniu. Import i eksport danych z systemów klasy BI do systemu ERP. Obsługa zestawień w module BI dostarczonym przez producenta. Wsparcie techniczne użytkowników w zakresie działania oprogramowania.
e. **Oprogramowanie „Kadry-Płace" + portal „HRP" (Asseco)** – zarządzanie i wsparcie użytkowników, synchronizacja danych, instalacja/wdrożenie wersji graficznych modułów.
f. **System KRDK (Krajowy Rejestr Dawców Krwi)** – obsługa portalu, wsparcie przy wyjaśnianiu zgłoszeń, weryfikacja poprawności działania importu oraz eksportu danych w ramach komunikacji obu systemów. Współpraca z innymi podmiotami odpowiedzialnymi za komunikację w ramach Krajowego Rejestru Dawców Krwi.
g. system EZD RP (Elektroniczne Zarządzanie Dokumentacją Rzeczypospolitej Polskiej) – wdrożenie i nadzór nad obiegiem dokumentacji elektronicznej w szarej strefie.
h. **Oprogramowanie klasy BI – „Cognos Analytycs" (IBM)** – wykonywanie zestawień na żądanie Zamawiającego. Administracja systemem, uprawnieniami, konfiguracją oraz harmonogramem wykonywanych raportów.
i. **Portal pracy grupowej / intranet (Microsoft SharePoint)** – administrowanie i zarządzanie systemem obiegu dokumentacji.
j. **Oprogramowanie klasy NMS – „nVision" (Axence)** – obsługa, konfiguracja, monitorowanie, raportowanie na żądanie Zamawiającego.
k. System replikacji danych - Assure Mimix (Precisely) – administrowanie systemem, wykonywanie operacji zamiany ról środowisk on-line, analiza logów oraz bieżąca weryfikacja poprawności działania replikacji.
l. **Systemy BMS** – w zakresie utrzymania i podstawowej administracji.
m. **Systemy IBM (OS serii IBM, IBM i Access for Windows)** – instalacja klienta, konfiguracja połączeń i sesji drukarkowych do Banku Krwi.

Szczegółowy wykaz infrastruktury i oprogramowania zawarty jest w punkcie 1 Opisu Przedmiotu Zamówienia.

3. Pozostałe obowiązki

a. Wsparcie użytkowników systemów informatycznych Zamawiającego (zdalnie, telefonicznie i lokalnie).
b. Udział we wdrażaniu nowych modułów i systemów, w tym walidacja systemów, zgodnie z procedurami Zamawiającego.
c. Prowadzenie szkoleń i instruktaży grupowych i indywidualnych dla pracowników w zakresie obsługi sprzętu oraz programów biurowych, aplikacji medycznych i specjalistycznych serwisów internetowych – poprzez szkolenia i bezpośrednie interwencje na stanowiskach roboczych. Liczba i zakres szkoleń uzależnione jest od bieżących potrzeb Zamawiającego, w okresie ostatnich 12 miesięcy było to ok. 5 szkoleń. Szkolenia odbywały się stacjonarnie w siedzibie głównej, jak również w formie online
d. Wykonawca obejmuje obowiązki Administratora Systemów Informatycznych w infrastrukturze Zamawiającego, w tym będzie wdrażał polityki bezpieczeństwa w uzgodnieniu z Inspektorem Ochrony Danych wyznaczonym przez Zamawiającego, zgodnie z obowiązującymi przepisami prawa, w szczególności przepisami o ochronie danych osobowych. Wykonawca będzie ponadto tworzył, prowadził, aktualizował niezbędną dokumentację oraz wykonywał inne czynności wynikające z roli Administratora Systemów Informatycznych, w tym nadzór nad dostępami użytkowników ich okresową weryfikacje we współpracy z kierownikami KO/TO jak i prowadzenie ewidencji osób upoważnionych, monitorowanie działania systemów oraz zgłaszanie i obsługę incydentów;
e. przestrzegał i działał zgodnie z procedurami i regulacjami wewnętrznymi Zamawiającego.
f. Przestrzeganie wewnętrznych procedur i regulaminów np. dotyczących zamówień publicznych w tym planowania wszystkich wydatków w obszarze IT;
g. Wsparcie zespołu ds. Systemu Zarządzania Bezpieczeństwem Informacji;
h. Współpraca z Inspektorem ds. Obronnych i Informacji Niejawnych

4. Reprezentowanie Zamawiającego

Wykonawca zobowiązuje się do reprezentowania na żądanie Zamawiającego wobec producentów / dostawców systemów (m.in. Asseco, BPX, CEZ, dostawcy UTM, dostawcy sprzętu) w zakresie zgłoszeń, eskalacji, uzgodnień technicznych i aktualizacji. Wykonawca w porozumieniu z Zamawiającym zobowiązuje się do udziału w szkoleniach merytorycznych dotyczących kluczowych systemów funkcjonujących w infrastrukturze Zamawiającego. Wykonawca zobowiązuje się do składania wyjaśnień i wprowadzania zaleceń w ramach kontroli podmiotów zewnętrznych przeprowadzanych u Zamawiającego.

Wykonawca zobowiązuje się do realizacji innych poleceń Zamawiającego, pozostających w związku z przedmiotem umowy, w szczególności w zakresie przygotowywania wyjaśnień, opinii oraz projektów odpowiedzi na pisma kierowane do Zamawiającego przez organy administracji publicznej, w tym Ministerstwo Zdrowia.

5. Dokumentacja i IOD

a. Wykonawca w trakcie trwania umowy, zobowiązuje się sporządzać i aktualizować dokumentację środowiska sieciowo sprzętowego w formie pozwalającej na przejęcie obsługi przez Zamawiającego lub inny podmiot po wygaśnięciu umowy. Wykonawca 30 dni przed końcem wygaśnięcia umowy przekaże Zamawiającemu komplet poświadczeń administracyjnych do systemów nad którymi sprawował nadzór.
b. Wykonawca zdeponuje w formie papierowej w sejfie lub innym bezpiecznym miejscu (gabinet Dyrektora Centrum) wszelkie hasła dostępowe, uwierzytelniające, administracyjne (root) do wszystkich zasobów ICT w ciągu 30 dni od dnia podpisania umowy.
c. Wykonawca zobowiązuje się do przestrzegania wszystkich obowiązujących u Zamawiającego dokumentów dotyczących ochrony danych, bezpieczeństwa informacji oraz zarządzania systemami, a także do aktywnej współpracy z Inspektorem Ochrony Danych.

6. Czas reakcji i usunięcia awarii/problemu

Zamawiający ustanawia następujące maksymalne czasy reakcji na zgłoszoną awarię/zgłoszenie oraz terminy usunięcia awarii lub problemu od momentu zgłoszenia:

Dla awarii krytycznych:

- Czas reakcji na zgłoszoną awarię – niezwłocznie, nie później niż do 2 godziny od zgłoszenia;
- Czas usunięcia awarii – do 6 godzin od zgłoszenia, z wyjątkiem systemów objętych wsparciem lub gwarancją innych podmiotów,
- Czas przywrócenia do stanu sprzed awarii pierwotnej – do 10 dni od zgłoszenia.

Dla pozostałych zgłoszeń:

- Czas reakcji na zgłoszoną awarię – do 12 godzin od zgłoszenia;
- Czas usunięcia awarii – do 72 godziny od zgłoszenia z wyjątkiem systemów objętych wsparciem lub gwarancją innych podmiotów.
- Czas przywrócenia do stanu sprzed awarii pierwotnej – do 14 dni od zgłoszenia.

7. Realizacja

Usługi będą realizowane w siedzibie Zamawiającego przy ul. Rzeźniczej 11 w Krakowie, a także zdalnie – dla terenowych oddziałów, z wyłączeniem sytuacji wymagających fizycznej obecności Wykonawcy w danym oddziale. Świadczenie usługi realizowane jest całą dobę we wszystkie dni, przy czym Wykonawca w godzinach 7:30–15:05 w dni robocze (tj. poniedziałek – piątek) zapewni obecność co najmniej 2 pracowników w siedzibie Zamawiającego (za wyjątkiem sytuacji wymagających fizycznej obecności w terenowych oddziałach kiedy w siedzibie musi pozostawać co najmniej 1 pracownik). Wykonawca zapewni dyżur telefoniczny – w dni robocze po godzinie 15:05 oraz w soboty i dni ustawowo wolne od pracy, zgodnie z ustalonymi czasami reakcji.

Wykonawca zapewni zdalną obsługę informatyczną w czasie weekendowych i świątecznych wyjazdowych akcji krwiodawstwa.

Zamawiający informuje również, że w porze nocnej odbywają się takie prace jak:

- Praca przy infrastrukturze teleinformatycznej (urządzenia dostępowe, zasilanie awaryjne) – 8 razy w ciągu roku po ok. 6 godzin

- aktualizacja systemu Banku Krwi – konieczna obecność osoby merytorycznej ze strony RCKiK (informatyka) przy aktualizacjach i przepięciach wersji – 5 razy w ciągu roku po ok. 8 godzin / tylko przepięcia BK to max dwa razy rok
- 1 raz na kwartał zamiana ról serwerów – produkcyjny / zapasowy w godzinach 21:00 – 2:00 – 4 razy w ciągu roku.

Zgłoszenia przekazywane będą drogą telefoniczną, mailową lub przez dedykowane rozwiązanie do obsługi zgłoszeń pomocy technicznej udostępnione przez Wykonawcę.

Terenowe Oddziały RCKiK w Krakowie:

Terenowy Oddział ul. Wielicka 265, 30-663 Kraków,

Terenowy Oddział os. Na Skarpie 66a, 31-913 Kraków,

Terenowy Oddział ul. Szpitalna 2, 32-400 Myślenice

Terenowy Oddział ul. Wysokie Brzegi 4, 32-600 Oświęcim,

Terenowy Oddział ul. Karolina 14C, 32-700 Bochnia,

Terenowy Oddział ul. Szpitalna 13, 33-100 Tarnów,

Terenowy Oddział ul. Lwowska 178A, 33-100 Tarnów,

Terenowy Oddział ul. Szpitalna 22, 34-200 Sucha Beskidzka

Terenowy Oddział ul. Szpitalna 14, 34-400 Nowy Targ

Terenowy Oddział ul. Szymony 14, 34-500 Zakopane

Terenowy Oddział ul. Piłsudskiego 61, 34-600 Limanowa

Terenowy Oddział ul. Węgierska 21, 38-300 Gorlice

Terenowy Oddział os. Kopernika 10/6, 34-100 Wadowice

Terenowy Oddział ul. Henryka Sienkiewicza 55, 33-300 Nowy Sącz