Załącznik nr 1 do Umowy CeZ/…/2023

OPIS PRZEDMIOTU ZAMÓWIENIA

Rozbudowa systemu PAM o licencje CyberArk Identity Enterprise lub równoważne.

1. **Przedmiot zamówienia obejmuje:**

1.1. Dostawę 1000 licencji CyberArk Identity Enterprise w modelu subskrypcyjnym wraz ze wsparciem producenta/Wykonawcy na okres 12 miesięcy od dnia podpisania przez Zamawiającego protokołu odbioru tych licencji);

1.2. Zamawiający posiada środowisko systemu bezpieczeństwa kont uprzywilejowanych (PAM- Privileged Access Management), na które składają się następujące licencje:

LP	Nazwa licencji	Liczba licencji
1.	CyberArk Privileged User Subscription PRIV-STANDARD-USER-SUBS	310

1.3. Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego wymagania wskazane do Załączniku nr 1 do OPZ. W przypadku dostarczania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w Opisie przedmiotu zamówienia.

2. **Termin realizacji:**

Dostawa zamówienia gwarantowanego, o którym mowa w pkt 1.1 musi nastąpić w terminie do 10 dni roboczych od zawarcia umowy.

3. **Wsparcie producenta/Wykonawcy:**

3.1. W ramach wsparcia producenta/Wykonawcy wymagany jest:

3.1.1. dostęp do aktualizacji oprogramowania;

3.1.2. dostęp do nowych wersji oprogramowania oraz poprawek;

3.1.3. dostęp do nowych sygnatur bezpieczeństwa;

3.1.4. dostęp do bazy wiedzy producenta

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Załączniku nr 1 do OPZ:

1. Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego wymagania w szczególności w zakresie:
    a) warunków licencji/sublicencji w każdym aspekcie licencjonowania/sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla posiadanego przez Zamawiającego oprogramowania,

    b) funkcjonalności rozwiązania równoważnego, która nie może być gorsza od funkcjonalności wymienionych w niniejszym Załączniku,

    c) rozwiązanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem PAM CyberArk funkcjonującym u Zamawiającego,

    d) rozwiązanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,

    e) rozwiązanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie i systemy informatyczne,

    f) rozwiązanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność rozwiązania równoważnego z wyspecyfikowanym systemem.

2. Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego następujące wymagania:
    a) System bezpieczeństwa kont uprzywilejowanych PAM (zwany dalej „Systemem") musi realizować funkcję:

    - wieloskładnikowego adaptacyjnego uwierzytelnienia.
    - zabezpieczenia dostępu zarówno do wewnętrznych jak i zewnętrznych aplikacji (SaaS) poprzez wykorzystanie zabezpieczonego portalu SSO.
    - zarządzania cyklem życia tożsamości (ang. lifecycle management, wymagający dodatkowej licencji czasowej).
    - przechowywania poświadczeń użytkownika biznesowego w centralnym repozytorium zainstalowanym w środowisku Zamawiającego. Wymagane jest, aby poświadczenia użytkowników w ramach repozytorium składowane były w formacie zaszyfrowanym przy wykorzystaniu zarówno kluczy symetrycznych, nie mniej niż AES256, jak również asymetrycznych, nie mniej niż RSA2048. Musi istnieć możliwość integracji z systemem CyberArk PAM na potrzeby realizacji tego wymagania.
    - Uwierzytelniania do systemu operacyjnego podczas logowania użytkownika. Wymagane jest wsparcie systemów operacyjnych nie mniej niż Microsoft Windows oraz MacOS.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

b) System musi być dostarczony jako usługa zewnętrzna (SaaS) wraz z modułem konektora, umożliwiającym integrację ze środowiskiem usług katalogowych AD/LDAP oraz uruchomienie serwera Radius dla klientów sieciowych Zamawiającego.

c) System nie może ograniczać licencyjnie liczby konektorów możliwych do zainstalowania w środowisku Zamawiającego.

d) System musi wspierać obsługę języka polskiego minimum dla interfejsu użytkownika i aplikacji mobilnej dostępnej dla systemów operacyjnych Android i iOS.

e) System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu SSO, pozwalający na realizację dla dowolnej aplikacji web nie mniej niż następujących funkcjonalności:

- rejestrowanie wszystkich działań użytkowników z wykorzystaniem podejścia „krokowego". System musi wywoływać zrzut ekranu okna przeglądarki użytkownika wraz z odpowiednimi metadanymi dla co najmniej następujących czynności wykonywanych przez użytkownika podczas monitorowanej sesji internetowej: kliknięcie myszką, naciśnięcie klawiszy „enter" lub „tab". System musi umożliwiać wyszukiwanie wszystkich nagranych sesji za pomocą dowolnego wprowadzania tekstu oraz filtrowanie zdarzeń związanych z bezpieczeństwem według dat i działań.
- zidentyfikowanie, kiedy sesja wysokiego ryzyka pozostaje otwarta i wymaga ponownego uwierzytelnienia, aby upewnić się, że osoba, która zainicjowała sesję internetową, jest osobą uprawnioną,
- ochronę sesji internetowej na punkcie końcowym za pomocą rozszerzenia przeglądarki,
- kontrolowanie wartości wprowadzanych przez użytkownika do pól tekstowych aplikacji web.

f) System musi umożliwiać generowanie incydentów w przypadku wykrycia nadużyć, dla nie mniej niż następujących sytuacji: wartość liczbowa wprowadzona przez użytkownika przekracza zdefiniowany w systemie próg, użytkownik przechodzi do miejsca w aplikacji, które jest szczególnie wrażliwe i zbudowana dla niego została polityka monitorująca. Jako reakcje na incydenty systemu musi udostępniać nie mniej niż: oznaczenie zdarzenia w systemie monitoringu sesji web, wysłanie powiadomienia na zdefiniowany adres email, wysłanie powiadomienia typu push do aplikacji mobilnej wybranego użytkownika. Tworzenie reguł musi być możliwe poprzez wykorzystanie pluginu zainstalowanego w przeglądarce administratora, bez konieczności dostępu do interfejsu graficznego rozwiązania.

g) System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu SSO, pozwalający na realizację dla dowolnej aplikacji web funkcjonalności certyfikacji dostępu umożliwiającej przeprowadzanie cyklicznych kampanii mających na celu automatyzację procesu nadawania i odwoływania dostępu użytkownika na podstawie procesu akceptacyjnego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

h) System musi zapewniać funkcjonalność certyfikacji dostępu (poprzez dodatkową subskrypcję, nieuwzględnioną w obecnej fazie projektu) w celu automatycznej weryfikacji, nadawania lub cofania uprawnień, jakie użytkownik posiada w systemie CyberArk PAM.

i) System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu SSO, pozwalający na realizację dla aplikacji funkcjonalności: zarządzania cyklem życia użytkownika, polegającej na pobieraniu atrybutów konta użytkownika z systemu HR (wymagane jest wsparcie dla nie mniej niż BambooHR, SAP SuccessFactors, Workday, UltiPro) i przekazaniu ich do docelowej aplikacji web w ramach procesu tworzenia konta nowego użytkownika.

j) System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu SSO, pozwalający na realizację integracji pomiędzy różnymi systemami źródłowymi i docelowymi, rozumianą jako możliwość pobrania danych wejściowych z systemu źródłowego (np. z wykorzystaniem API) i przekazania ich z zmienionej lub zmodyfikowanej formie do systemu docelowego (np. również z wykorzystaniem API). System musi udostępniać interfejs użytkownika umożliwiających opisanie wymaganych przepływów danych w ujęciu no-code (bez konieczności opisywania wymaganych założeń za pomocą języków skryptowych). System musi wspierać integrację z wiodącymi technologiami cyberbezpieczeństwa i rozwiązaniem PAM CyberArk z wykorzystaniem gotowych szablonów integracji dostępnych w formie out of the box.

k) System musi zapewniać dodatkowy komponent (poprzez dodatkową subskrypcję, nieuwzględniony w obecnej fazie projektu) jako rozszerzenie modułu MFA, pozwalający na realizację silnego uwierzytelniania wieloskładnikowego na poziomie systemu operacyjnego, wymuszanego podczas podnoszenia uprawnień oraz uruchamiania aplikacji realizowanego przez użytkownika. Warunki wymuszające egzekwowanie MFA muszą być opisane w ramach polityki powiązanej z kontrolą aplikacji uruchamianych na systemie operacyjnym. Wymagana jest możliwość budowanie polityki kontrolującej aplikacje w oparciu o warunki dopasowujące nie mniej niż: Filename, Checksum, Parameters, Location type, Owner, Product name, File description, Company name, Original filename, File version, Product version, Source, Parent process. Wymagane jest wsparcie dla nie mniej niż następujących systemów operacyjnych: Windows 7 x32 & x64, Windows 8/8.1 x32 & x64, Windows 10 x32 & x64, Windows 11 x64, Windows Server 2008 x32 & x64, Windows Server 2008 R2 x64, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, macOS Big Sur 11, macOS Monterey 12, macOS Ventura 13.

l) Wymagana jest możliwość obsługi minimum następujących składników uwierzytelniających: hasło, sms, email, oauth, aplikacja mobilna, phone call, pytanie bezpieczeństwa, składniki kompatybilne ze standardem Fido2 (np. token sprzętowy, Windows hello, touch id), certyfikat użytkownika, karta PIV/CAC, Qrcode generowany w ramach procesu uwierzytelnienia do interfejsu Systemu i systemu operacyjnego (umożliwiający uwierzytelnienie użytkownika przy użyciu aplikacji mobilnej uprzednio zarejestrowanej w systemie).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

m) System musi wspierać kontekstowe uwierzytelnianie bazujące na minimum następujących warunkach: adres IP, dzień tygodnia, data, zakres dat, zakres czasu, adaptacyjnie poprzez automatyczną analizę zachowań użytkowników (profilowanie urządzenia, adresu IP, śledzenia zagrożeń poprzez funkcję "Threat Intelligence").

n) Moduł MFA poprzez protokół Radius musi umożliwiać integrację z popularnymi koncentratorami VPN.

o) System musi posiadać edytor graficzny do tworzenia niestandardowych przepływów uwierzytelniania, umożliwiający tworzenie reguł uwierzytelniania, z nie mniej niż następującymi możliwościami:

- możliwość zbudowania przepływu uwierzytelniania do portalu użytkownika, wymuszającego wskazaną kombinacje składników uwierzytelniających w oparciu o warunki typu if-else (mechanizm ten musi umożliwiać szczegółowe definiowanie zależności np. jeśli użytkownik jako pierwszy składnik wybierze hasło, jako drugi składnik musi wybrać otp, natomiast jeśli jako pierwszy składnik wybierze aplikację mobilną – nie będzie poproszony o drugi składnik. W przeciwnych wypadkach wymagane będzie uwierzytelnianie w oparciu o QRCode) i filtry (nie mniej niż adres IP, plik cookie, dzień tygodnia, data, zakres dat, zakres czasowy, System operacyjny urządzenia, przeglądarka, kraj, poziom ryzyka, uwierzytelnianie certyfikatu).

- aplikacje internetowe, możliwość zbudowania przepływu uwierzytelniania, wymuszającego wskazaną kombinacją składników uwierzytelniających w oparciu o warunki typu if-else (mechanizm ten musi umożliwiać szczegółowe definiowanie zależności np. jeśli użytkownik jako pierwszy składnik wybierze hasło, jako drugi składnik musi wybrać otp, natomiast jeśli jako pierwszy składnik wybierze aplikację mobilną – nie będzie poproszony o drugi składnik. W przeciwnych wypadkach wymagane będzie uwierzytelnianie w oparciu o QRCode) i filtry (nie mniej niż adres IP, plik cookie uwierzytelniania, dzień tygodnia, data, zakres dat, zakres czasu, system operacyjny urządzenia, Przeglądarka, Rola, Kraj, Zarządzane urządzenie, Poziom ryzyka, Uwierzytelnianie certyfikatu).

- ogólny profil uwierzytelniania, możliwość zbudowania przepływu uwierzytelniania, wymuszającego wskazaną kombinacją składników uwierzytelniających w oparciu o warunki typu if-else (mechanizm ten musi umożliwiać szczegółowe definiowanie zależności np. jeśli użytkownik jako pierwszy składnik wybierze hasło, jako drugi składnik musi wybrać otp, natomiast jeśli jako pierwszy składnik wybierze aplikację mobilną – nie będzie poproszony o drugi składnik. W przeciwnych wypadkach wymagane będzie uwierzytelnianie w oparciu o QRCode) i filtry.

p) System musi udostępniać aplikację do generowania kodów OTP dostępną dla systemu operacyjnego Windows. Podczas uruchamiania aplikacja po zarejestrowaniu musi wymuszać od użytkownika podaniu kodu PIN zdefiniowanego podczas procesu rejestracji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

q) System musi posiadać wbudowane narzędzie obrazujące na bieżąco minimalny i maksymalny poziom AAL (Authenticator Assurance Level) możliwy do uzyskania za pomocą składników uwierzytelniających wybranych w profilu uwierzytelniającym.

r) System musi posiadać moduł integracji z systemem ADFS umożliwiający wymuszanie mechanizmu MFA bez konieczności modyfikacji zintegrowanej aplikacji.

s) System musi posiadać wbudowany moduł analizujący zachowanie i profilowanie użytkownika w oparciu o nie mniej niż następujące parametry: historia profilu logowania, charakterystyka godzin i dni tygodnia logowań, charakterystyka zmian geolokalizacyjnych użytkownika, obecność zaufanego certyfikatu na urządzeniu, z którego zestawiane jest połączenie, lokalizacja z której realizowane jest połączenie. W zależności od wyliczonego poziomu ryzyka musi istnieć możliwość przypisania odpowiednich profili uwierzytelniających oraz blokowania dostępu.

t) System musi umożliwiać wysłanie powiadomień o wystąpieniu ryzykownych zdarzeń z wykorzystaniem webhook.

u) System musi posiadać ochronę przed atakami klasy phishing (potwierdzenie, iż użytkownik loguje się do odpowiedniego portalu) poprzez wybór przez użytkownika końcowego obrazka wyświetlanego przy każdym logowaniu do portalu.

v) Platforma SaaS musi posiadać certyfikację SOC2 Type 2.

w) System musi realizować usługę SSO dla aplikacji chmurowych oraz wewnętrznych, realizując w sposób scentralizowany bezpieczne uwierzytelnienie przy wykorzystaniu metod opisanych w Załączniku nr 1 do OPZ, punkcie 2, w podpunktach od l do v. Musi istnieć możliwość integracji z własnymi aplikacjami poprzez nie mniej niż następujące integracje:

- plugin do przeglądarki
- NTLM
- Basic auth
- Klient Oauth2
- Serwer Oauth2
- OpenID Connect
- Saml
- WS-Fed
- Użytkownik – hasło

x) System musi posiadać gotowe integracje SSO z nie mniej niż następującymi aplikacjami: Adobe Sign, Amazon Web Services, Box, Dropbox, NetSuite, Office 365, Salesforce, ServiceNow, Slack, Webex, Zendesk.

y) Dla użytkowników zewnętrznych którzy chcą skorzystać z aplikacji web w centrum danych Zamawiającego System musi posiadać funkcję (dostępną w ramach dodatkowej licencji czasowej) nawiązania bezpiecznego połączenia bez konieczności zestawiania dodatkowych tuneli VPN pomiędzy stacją roboczą a centrum danych (realizować funkcję reverse proxy).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

z) Dla aplikacji web, które nie wspierają protokołów SSO (jak SAML) musi istnieć możliwość integracji z wykorzystaniem uwierzytelniania w oparciu o nazwę użytkownika i hasło. Dla tego typu aplikacji użytkownik musi mieć możliwość samodzielnego podania w systemie danych uwierzytelniających. Podczas połączenia plugin zainstalowany w przeglądarce użytkownika musi dokonywać procesu automatycznego uzupełniania poświadczeń we właściwe pola aplikacji web. System musi umożliwiać składowanie poświadczeń wprowadzonych przez użytkownika w centralnym repozytorium zainstalowanym w środowisku Zamawiającego. Wymagane jest, aby poświadczenia użytkowników w ramach repozytorium składowane były w formacie zaszyfrowanym przy wykorzystaniu zarówno kluczy symetrycznych, nie mniej niż AES256, jak również asymetrycznych, nie mniej niż RSA2048. Musi istnieć możliwość integracji z systemem CyberArk PAM na potrzeby realizacji tego wymagania.

aa) System musi automatycznie rozpoznawać wizyty na nowych stronach web, gdzie użytkownik zostanie poproszony o uwierzytelnienie. Dane uwierzytelniające podane przez użytkownika muszą zostać przechwycone i zapisane w repozytorium haseł oraz odpowiednia nowa aplikacja web musi zostać dodana do katalogu aplikacji w portalu SSO. System musi umożliwiać składowanie poświadczeń wprowadzonych przez użytkownika w centralnym repozytorium zainstalowanym w środowisku Zamawiającego. Wymagane jest, aby poświadczenia użytkowników w ramach repozytorium składowane były w formacie zaszyfrowanym przy wykorzystaniu zarówno kluczy symetrycznych, nie mniej niż AES256, jak również asymetrycznych, nie mniej niż RSA2048. Musi istnieć możliwość integracji z systemem CyberArk PAM na potrzeby realizacji tego wymagania.

bb) System musi umożliwiać składowanie poświadczeń oraz notatek wprowadzonych przez użytkownika w centralnym repozytorium zainstalowanym w środowisku Zamawiającego. Wymagane jest, aby poświadczenia użytkowników w ramach repozytorium składowane były w formacie zaszyfrowanym przy wykorzystaniu zarówno kluczy symetrycznych, nie mniej niż AES256, jak również asymetrycznych, nie mniej niż RSA2048. Musi istnieć możliwość integracji z systemem CyberArk PAM na potrzeby realizacji tego wymagania.

cc) System musi umożliwiać udostępnienie przez użytkownika (właściciela) poświadczeń i notatek innemu użytkownikowi lub grupie użytkowników.

dd) System musi zapewnić wtyczkę do przeglądarki użytkownika z wbudowaną funkcją generatora haseł. Generator haseł musi umożliwiać określenie co najmniej długości hasła i stopnia złożoności nowo generowanego hasła (system musi umożliwiać wybór, czy w nowo generowanym haśle mają być użyte cyfry, symbole, wielkie i małe litery).

ee) System musi umożliwiać zdefiniowanie mechanizmu TOTP w interfejsie graficznym systemu dla aplikacji web które wymagają TOTP podczas procesu uwierzytelniania. Właściciel biznesowy aplikacji wraz ze zdefiniowany TOTP oraz administrator systemu muszą mieć możliwość udostępnienia zintegrowanego z aplikacją web TOTP innym użytkownikom.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

ff) System musi posiadać możliwość definiowania w interfejsie nowego właściciela aplikacji oraz poświadczeń, umożliwiający tym samym dostęp w przypadku gdy dotychczasowy właściciel opuści organizację.

gg) Poprzez dodatkowe rozszerzenie licencyjne system musi realizować funkcję MFA wymuszane na chronionych serwerach Windows przy połączeniu uprzywilejowanym realizowanym w oparciu o moduł proxy systemu PAM CyberArk. W ramach realizacji połączenia uprzywilejowanego moduł proxy musi auto uzupełnić poświadczenia i umożliwić użytkownikowi wpisanie kolejnego składnika MFA. Sesja musi być zestawiana w oparciu o koncepcję izolacji. System musi umożliwiać wymuszenie weryfikacji trzeciego składnika MFA na poziomie aplikacji mobilnej (minimum możliwe do zastosowania: PIN oraz uwierzytelnianie biometryczne).

hh) System musi realizować wieloskładnikowe uwierzytelnianie użytkownika do systemu operacyjnego podczas procesu logowania. Wymagane jest wsparcie dla składników uwierzytelniających nie mniej niż: hasło, sms, email, oauth, aplikacja mobilna, phone call, pytanie bezpieczeństwa, Qrcode, wymuszane zgodnie ze zdefiniowaną polityką i wyrażeniami if-else. Wymagane jest wsparcie dla systemu operacyjnego nie mniej Windows oraz MacOS.

3. W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane rozwiązanie równoważne.
4. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu rozwiązania równoważnego.
5. Rozwiązanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania i systemów informatycznych u Zamawiającego.
6. Rozwiązanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie rozwiązania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie rozwiązania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w Jego nowszych wersjach.
7. W przypadku dostawy rozwiązania równoważnego Wykonawca zobowiązany jest:
    a) Przeprowadzić Instruktaż dla 4 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania rozwiązaniem równoważnym, umożliwiającym pełne poznanie rozwiązania równoważnego. Wykonawca w terminie 1 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram Instruktażu.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

b) Przeprowadzić Instruktaż dla 8 operatorów Zamawiającego z zakresu użytkowania rozwiązania równoważnego, umożliwiającego pełne poznanie produktu równoważnego.

c) Wykonawca w terminie 1 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogramy Instruktaży.

d) Instruktaże będą realizowane w Dni Robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub w formie zdalnej o ile zostaną spełnione wszystkie wymagania dotyczące Instruktażu. Instruktaż będzie trwał minimum 2 dni robocze każdy (łącznie minimum 14 godzin zegarowych każdy).

e) Zainstalować rozwiązanie równoważne w środowisku systemowo-programowym oraz dokonać poprawnej konfiguracji mechanizmów systemu typu PAM oraz zintegrować się z systemami/aplikacjami wytwarzanymi w ramach działalności Zamawiającego w terminie do 3 dni roboczych od dnia podpisania Umowy.

f) Dostarczyć wszelkie dodatkowe licencje - niezbędne do prawidłowego funkcjonowania rozwiązania równoważnego.

g) Opracować i dostarczyć do zamawiającego dokumentację powykonawczą wdrożonego rozwiązania równoważnego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706