CENTRALNA
KOMISJA
EGZAMINACYJNA

Załącznik nr 1 do Ogłoszenia

OPIS PRZEDMIOTU ZAMÓWIENIA

Usługi wsparcia IT (0365, infrastruktura sieciowa)

Przedmiotem zamówienia jest:

1. wsparcie w zakresie użytkowania i administrowania usługami oraz infrastrukturą teleinformatyczną Centralnej Komisji Egzaminacyjnej;
2. dostawa i wdrożenie 150 sztuk licencji Azure Active Directory Premium P1 lub równoważnej;
3. szkolenie dla pracowników IT Zamawiającego z zakresu cyberbezpieczeństwa oraz zarządzania sieciami LAN/WAN.

Ad.1

1. Wykonawca jest zobowiązany zapewnić **wsparcie IT** (w tym wsparcie techniczne) w okresie **24 miesięcy** od dnia podpisania umowy, z zastrzeżeniem, że w pierwszym miesiącu trwania umowy Wykonawca przeprowadzi **przegląd** infrastruktury IT CKE.
2. W ramach przeglądu Wykonawca:
   1) dokona ewidencji (zestawienie tabelaryczne możliwe do otworzenia w programie MS Excel) i sprawdzi konfigurację 5 serwerów; 150-170 komputerów, w tym laptopów;
   2) dokona ewidencji (zestawienie tabelaryczne możliwe do otworzenia w programie MS Excel) i przeprowadzi analizę bezpieczeństwa urządzeń podłączonych do sieci Internet oraz wskaże potencjalne zagrożenia, luki w zabezpieczeniach a także zalecania w zakresie niwelowania ww. zagrożeń;
   3) dokona ewidencji (zestawienie tabelaryczne rodzaju i liczby posiadanego oprogramowania w tym licencji, możliwe do otworzenia w programie MS Excel) oraz:
      a) sprawdzi legalność posiadanego przez Zamawiającego oprogramowania oraz w przypadku wykrycia nielegalnego oprogramowania (brak lub niewłaściwa licencja do użytkowania) wskaże sprzęt, na którym zainstalowane jest to oprogramowanie wraz z przyczyną uznania go za nielegalne,
      b) uwzględni dane o terminach zakończenia poszczególnych licencji w zestawieniu, o którym mowa w pkt. 3a), oraz w okresie trwania umowy będzie uaktualniał zestawienie;
   4) opracuje raport podsumowujący przegląd zawierający co najmniej:

a) zestawienia, o których mowa w pkt. 1-3) (szczegółowe pola zestawień zostaną określone przez Zamawiającego po podpisaniu umowy);
b) opis metodologii przeglądu w zakresie bezpieczeństwa urządzeń – założenia i zakres przeprowadzonej analizy bezpieczeństwa urządzeń podłączonych do sieci Internet, w tym zakres zastosowanych metod i narzędzi użytych w celu wykrycia potencjalnych zagrożeń, luk w zabezpieczeniach;
c) wyniki przeglądu po zastosowaniu metodologii, o której mowa w pkt. b), w tym informacje na temat znalezionych zagrożeń wraz z wskazaniem urządzenia, którego zagrożenie dotyczy oraz propozycję sposobu ich eliminacji (konkretne zalecenia, jakie należy zastosować w celu eliminacji ryzyka).

Zamawiający zastrzega sobie prawo do wniesienia uwag do przedłożonego raportu w terminie 7 dni kalendarzowych od jego otrzymania. Wykonawca zobowiązany jest do uwzględnienia uwag oraz naniesienia poprawek w raporcie, w terminie 7 dni kalendarzowych od dnia zgłoszenia uwag przez Zamawiającego, jeżeli usuwają niezgodności ze stanem faktycznym.

3. Usługi **wsparcia technicznego** w zakresie infrastruktury teleinformatycznej CKE będą realizowane przez Wykonawcę w odpowiedzi na zgłoszenia przekazywane przez pracowników Zamawiającego, tj.:

1) zgłoszenia techniczne,

2) zgłoszenia awarii,

3) doradztwo techniczne,

w całym okresie realizacji umowy (24 miesiące), w godz. 8.00 - 18.00, 7 dni w tygodniu, 365 dni w roku, w trybie zgłoszenia telefonicznego, serwisu www udostępnionego przez Wykonawcę lub pocztą elektroniczną. Zamawiający wskaże priorytet zgłoszenia oraz opisze problem wymagający rozwiązania. Szczegółowe zasady dot. zgłoszeń (przekazania i potwierdzenia otrzymania) Wykonawca przedstawi Zamawiającemu nie później niż w dniu podpisania umowy.

Po przekazaniu zgłoszenia przez Zamawiającego Wykonawca jest zobowiązany w terminie do 15 minut od otrzymania zgłoszenia do potwierdzenia jego przyjęcia (przesłanie informacji Zamawiającemu o przyjęciu zgłoszenia wraz z nadanym numerem zgłoszenia).

Wykonawca jest zobowiązany rozwiązywać zgłoszone problemy w następującym zakresie:

Priorytet	Opis – minimalne wymagania	SLA
High (Wysoki)	Całkowita awaria usługi/systemu Zamawiającego (brak kluczowych funkcjonalności usługi)	do 6h na usunięcie awarii lub zaproponowanie obejścia od momentu przekazania zgłoszenia do Wykonawcy przez Zamawiającego z zastrzeżeniem, że usunięcie awarii lub obejście przywróci usługę/system w terminie do 24h do stanu pierwotnej funkcjonalności
Medium (Średni)	Awaria usługi/systemu dotycząca kluczowego personelu (dyrektorzy, kierownicy)	do 8h na usunięcie awarii lub zaproponowanie obejścia od momentu przekazania zgłoszenia do Wykonawcy przez Zamawiającego, z zastrzeżeniem, że usunięcie awarii lub obejście przywróci usługę/system w terminie do 48h do stanu pierwotnej funkcjonalności
Low (Niski)	Inne zgłoszenie dotyczące problemu/awarii usługi lub systemu	do 2 dni roboczych na rozwiązanie problemu/awarii usługi lub systemu od momentu przesłania zgłoszenia do Wykonawcy przez Zamawiającego
None (Bardzo Niski)	Zgłoszenie dotyczące prośby o informację lub zmiany standardowej konfiguracji	do 3 dni roboczych na udzielenie informacji lub zmianę konfiguracji od momentu przesłania zgłoszenia do Wykonawcy przez Zamawiającego

W procesie rejestrowania zgłoszenia (nadanie numeru zgłoszenia) Wykonawca jest uprawniony do oceny prawidłowości priorytetu zgłoszonego przez Zamawiającego.

W przypadku gdy Wykonawca oceni, że zgłoszony priorytet jest niewłaściwy, w potwierdzeniu przyjęcia zgłoszenia przekazuje Zamawiającemu informacje o zmianie priorytetu wraz z uzasadnieniem.

Zamawiający zastrzega sobie prawo do zmiany priorytetu zarejestrowanego zgłoszenia przez Wykonawcę, jeżeli ustalony przez Wykonawcę priorytet jest nieprawidłowy. Decyzja Zamawiającego jest w ww. wypadku ostateczna tj. obowiązują czasy SLA przypisane do priorytetu wskazanego przez Zamawiającego.

W uzasadnionych przypadkach Zamawiający może wyrazić zgodę na wydłużenie czasu SLA poszczególnych zgłoszeń. Wyrażenie zgody wymaga poinformowania Wykonawcy min. drogą mailową.

Czasy SLA liczone są w czasie pracy „biura" zgłoszeń Wykonawcy tj. w godz. 8.00 - 18.00.

W przypadku nie dotrzymania czasów SLA kary umowne będą liczone za każdą przekroczoną godzinę niezależnie od godzin pracy „biura" zgłoszeń. Wykonawca każdorazowo niezwłocznie informuje Zamawiającego o zamknięciu zgłoszenia (po rozwiązaniu zgłoszonego problemu) wraz z przesłaniem instrukcji rozwiązania problemu.

W przypadku, gdy Wykonawca nie prześle Zamawiającemu informacji o przyjęciu zgłoszenia wraz z nadanym numerem zgłoszenia czas SLA liczony jest od momentu przesłania zgłoszenia do Wykonawcy.

Wykonawca zobowiązany jest do raportowania zgłoszeń/zmian/awarii/SLA w trybie miesięcznym tj. na koniec każdego miesiąca. Raport zawiera co najmniej: nr zgłoszenia, opis problemu/awarii/zgłoszenia, czas zgłoszenia, czas rozwiązania.

4. **Usługi wsparcia IT** w zakresie użytkowania i administrowania usługami oraz infrastrukturą teleinformatyczną CKE obejmują pomoc przy:
   1) administrowaniu środowiskiem Office 365 między innymi w zakresie dodawania/usuwania kont, konfiguracji, przypisywania licencji;
   2) monitoringu platformy Microsoft 365 między innymi w zakresie kont użytkowników i posiadanych licencji, poprawnego działania systemów, wykrywania błędów i podatności;
   3) administrowaniu dwoma środowiskami wirtualizacyjnymi Vmware między innymi w zakresie ciągłości działania maszyn wirtualnych i monitorowaniu zasobów;

4) administrowaniu systemami backupowymi między innymi pomoc w tworzeniu backupu, pomoc przy testach odtworzenia backupu;
5) administrowaniu systemami bezpieczeństwa między innymi w monitorowaniu potencjalnych zagrożeń oraz wdrażaniu krytycznych poprawek w infrastrukturze teleinformatycznej Zamawiającego;
6) administrowaniu systemami informatycznymi Zamawiającego oraz koordynacji działań zapewniających sprawne funkcjonowanie i zabezpieczenie systemów informatycznych Zamawiającego przed niepowołanym dostępem;
7) administrowaniu oraz sprawowaniu nadzoru nad sieciami komputerowymi między innymi monitorowanie przepustowości sieci, oraz jakości sprzętu sieciowego, zapewnienie ciągłości działania infrastruktury Zamawiającego,
8) monitorowaniu systemów informatycznych oraz zapewnienie ciągłości ich pracy od strony technicznej;
9) bieżącym rozwiązywaniu problemów technicznych dotyczących rozwiązań teleinformatycznych Zamawiającego;
10) planowaniu rozwoju infrastruktury i środowiska teleinformatycznego (doradztwo) - doradzanie Zamawiającemu w zakresie doboru właściwego sprzętu i oprogramowania informatycznego, wg potrzeb Zamawiającego;
11) bieżącym aktualizowaniu oprogramowania urządzeń do najnowszej wersji stabilnej, zalecanej przez producenta;
12) przeprowadzaniu testów odtworzenia maszyn wirtualnych z kopii zapasowej na wydzielonym środowisku testowym. Testy odtworzenia maszyn wirtualnych odbywać się będą zgodnie z harmonogramem ustalonym przez strony, ale nie częściej niż raz na kwartał;
13) bieżącym prowadzeniu dokumentacji technicznej z zakresu prowadzonych prac konfiguracyjnych tj. tworzenie instrukcji rozwiązania problemu oraz opis przeprowadzonych działań w toku rozwiązania problemu. Instrukcja z rozwiązaniem danego problemu będzie przesyłana do Zamawiającego za każdym razem wraz z informacją o zamknięciu zgłoszenia;
14) wdrożeniu funkcjonalności dostępu warunkowego dla usług M365 tj. współtworzenie polityk zabezpieczających dostęp do zasobów chmurowych Zamawiającego z uwzględnieniem co najmniej poniższych wymagań:
    a) dostęp z urządzeń określonych jako urządzenia firmowe – zarówno telefony komórkowe jak i stacje końcowe użytkowników,

b) dostęp dla ról administracyjnych z określonych lokalizacji oraz wymagania dodatkowego składnika uwierzytelnienia- identyfikacja i konfiguracja wyjątków dla kont technicznych i usługowych;

15) wdrożeniu dodatkowego składnika uwierzytelnienia dla połączeń VPN i integracja z Active Directory Zamawiającego:
   a) integracja usługi VPN ze środowiskiem Active Directory – uwierzytelnienie kontem domenowym,
   b) konfiguracja przypisywania profili VPN na podstawie przynależności do grup Active Directory,
   c) konfiguracja dodatkowego uwierzytelnienia w formie certyfikatu pochodzącego z lokalnego centrum certyfikatów Zamawiającego.

Ad. 2

1. W terminie **4 miesięcy** od daty zawarcia umowy Wykonawca dostarczy i wdroży **150 sztuk** licencji Azure Active Directory Premium P1 lub równoważnej. Licencja równoważna musi spełniać poniższe wymagania:
   1) **Uwierzytelnianie, logowanie jednokrotne i uwierzytelnianie wieloskładnikowe (MFA):**
      - Uwierzytelnianie w chmurze (Uwierzytelnianie przekazujące, synchronizacja skrótu hasła);
      - Uwierzytelnianie federacyjne
      - Logowanie jednokrotne (SSO) bez ograniczeń
      - Uwierzytelnianie wieloskładnikowe (MFA)
      - Bez hasła (typu: Windows Hello dla firm, Microsoft Authenticator, integracje klucza zabezpieczeń FIDO2)
      - Umowa dotycząca poziomu usług
   2) **Dostęp aplikacji:**
      - Aplikacje typu SaaS z nowoczesnym uwierzytelnianiem
      - Przypisanie grupy do aplikacji
      - Odnajdowanie aplikacji w chmurze
      - Serwer proxy aplikacji dla lokalnego, opartego na nagłówku i zintegrowanego uwierzytelnienia systemu Windows
      - Partnerstwa w zakresie bezpiecznego dostępu hybrydowego
   3) **Autoryzacja i dostęp warunkowy:**
      - Kontrola dostępu na podstawie ról (RBAC)
      - Dostęp warunkowy

- Ograniczony dostęp do programu SharePoint
- Zarządzanie czasem życia sesji
- Niestandardowe atrybuty zabezpieczeń

4) **Administracja i tożsamość hybrydowa:**
   - Zarządzanie użytkownikami i grupami
   - Zaawansowane zarządzanie grupami (Grupy dynamiczne, zasady nadawania nazw, wygasanie, domyślna klasyfikacja)
   - Synchronizacja katalogów — (synchronizacja i synchronizacja w chmurze)
   - Raportowanie usługi stanu połączenia
   - Administracja delegowana — wbudowane role
   - Globalna ochrona hasłem i zarządzanie — użytkownicy tylko w chmurze
   - Globalna ochrona hasłem i zarządzanie — zabronione niestandardowo hasła, użytkownicy synchronizowani z lokalnej usługi Active Directory (posiadanej przez Zamawiającego).
5) **Samoobsługa użytkowników:**
   - Portal uruchamiania aplikacji
   - Kolekcje aplikacji użytkownika w portalu
   - Portal samoobsługowego zarządzania kontem
   - Samoobsługowa zmiana hasła dla użytkowników w chmurze
   - Samoobsługowe resetowanie haseł/zmienianie/odblokowywanie przy użyciu lokalnego zapisu zwrotnego
   - Samoobsługowe wyszukiwanie i raportowanie aktywności dotyczącej logowania
   - Samoobsługowe zarządzanie grupą
6) **Zarządzanie tożsamościami:**
   - Zautomatyzowana aprowizacja użytkowników w aplikacjach
   - Zautomatyzowana aprowizacja grup w aplikacjach
   - Aprowizowanie sterowane przez kadry
   - Zaświadczanie warunków użytkowania
7) **Rejestrowanie zdarzeń i raportowanie:**
   - Podstawowe raporty dotyczące zabezpieczeń i użycia
   - Zaawansowane raporty dotyczące zabezpieczeń i użycia
8) **Pracownicy pierwszego kontaktu:**
   - Logowanie przy użyciu wiadomości SMS
   - Wylogowywanie się z urządzenia udostępnionego
   - Portal zarządzania użytkownikiem delegowanym

2. **Wdrożenie licencji** obejmuje:
   1) integrację przypisania licencji na podstawie grup Active Directory;
   2) wdrożenie mechanizmu samodzielnego resetu hasła użytkownika wraz z synchronizacją wsteczną do Active Directory;
   3) wdrożenie mechanizmu ochrony haseł.

Ad. 3

1. Przygotowanie i przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa oraz zarządzania sieciami LAN/WAN:
   1) W trakcie trwania umowy w terminie wskazanym przez Zamawiającego, Wykonawca przeprowadzi szkolenie IT dla pracowników Zamawiającego (6 osób) w zakresie zarządzania sieciami LAN, WAN oraz w zakresie cyberbezpieczeństwa, w siedzibie Zamawiającego. Czas trwania szkolenia: minimum 64 godziny. Wykonawca zapewni połączenie szkoleń z warsztatami.
   2) Wykonawca jest zobowiązany przygotować dla każdego uczestnika szkolenia materiały szkoleniowe w wersji elektronicznej lub papierowej wg decyzji Zamawiającego.
   3) Wykonawca zobowiązany jest na 7 dni roboczych przed rozpoczęciem szkolenia przedłożyć Zamawiającemu program i harmonogram szkolenia.
   4) Program szkolenia musi zawierać m. in. aktualne potrzeby rynku IT, uwzględniać aktualne trendy w zakresie przedmiotowych umiejętności i kwalifikacji zawodowych, uwzględniać rekomendacje ekspertów na rynku IT, tak aby w jak największym stopniu umożliwiać uczestnikom uzyskanie i/lub uzupełnianie praktycznej wiedzy i umiejętności oraz kwalifikacji zawodowych.

Kody CPV:

1. Kod główny:

   72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia;

2. Kody dodatkowe:

   48000000-8 Pakiety oprogramowania i systemy informatyczne;
   72246000-1 Usługi doradcze w zakresie systemów;
   72250000-2 Usługi w zakresie konserwacji i wsparcia systemów;
   72253200-5 Usługi w zakresie wsparcia systemu;
   72720000-3 Usługi w zakresie rozległej sieci komputerowej;
   80000000-4 Usługi edukacyjne i szkoleniowe.

Zespół Obsługi Informatycznej
Kaczyński
Rafał Kaczyński
SAMODZIELNY REFERENT