Łódź dnia 12.05.2022 r.

Prezes Biura do spraw Substancji Chemicznych z siedzibą w Łodzi,

ul. Dowborczyków 30/34

ZAPRASZA DO ZŁOŻENIA PROPOZYCJI CENOWEJ na usługę

hostingu dedykowanego wraz z łączem telekomunikacyjnym podłączonym do sieci Internet, odpowiednim oprogramowaniem systemowym oraz usługą serwisową, konserwacyjną i administracyjną serwerów i firewall'a dla Biura do spraw Substancji Chemicznych.

1. Opis sposobu przygotowania propozycji cenowej:
   a) Musi być napisana w języku polskim, czytelną i trwałą techniką.
   b) Ceny w niej podane mają być wyrażone cyfrowo i słownie.
   c) Ma obejmować całość zamówienia.
2. Opis przedmiotu zamówienia:

   Przedmiotem zamówienia jest usługa hostingu dedykowanego wraz z łączem telekomunikacyjnym podłączonym do sieci Internet, odpowiednim oprogramowaniem systemowym oraz usługą serwisową, konserwacyjną i administracyjną serwerów i firewall'a dla Biura do spraw Substancji Chemicznych..

   Szczegółowy opis przedmiotu zamówienia znajduje się w Załączniku nr 1 do Zaproszenia.
3. Wymagany termin realizacji zamówienia: do 01.06.2022 r.
4. Przy wyborze propozycji do realizacji, Zamawiający będzie się kierował kryterium:
   a) Cena – 100 %
5. Propozycja cenowa składana przez Wykonawcę powinna zawierać następujące dokumenty:
   5.1 Formularz propozycji cenowej wg załączonego wzoru (Załącznik 3).
   5.2 Kserokopię lub wydruk aktualnego wpisu do rejestru uprawniającego Wykonawcę do występowania w obrocie prawnym, a w przypadku prowadzonej działalności gospodarczej zaświadczenie lub wydruk z Centralnej Ewidencji Działalności Gospodarczej.
   5.3 Oświadczenie Wykonawcy, że spełnia następujące warunki (Załącznik 2):
   a) Jest uprawniony do występowania w obrocie prawnym, zgodnie z wymogami ustawowymi.
   b) Posiada niezbędną wiedzę i doświadczenie oraz dysponuje potencjałem technicznym i osobami zdolnymi do wykonania zadania.
   c) Znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zadania.
6. Miejsce i termin złożenia propozycji cenowej:

Propozycję cenową należy złożyć do dnia 20.05.2022 r. do godz. 12.00.

Propozycja cenowa może zostać przesłana za pośrednictwem poczty elektronicznej na adres: **zp@chemikalia.gov.pl**

7. Osobami uprawnionymi do kontaktu z Wykonawcą są:

p. Przemysław Cieśla– pciesla@chemikalia.gov.pl, tel. 42 2538406

p. Dorota Smykowska – dsmykowska@chemikalia.gov.pl, tel. 42 2538400

8. **Informacje dotyczące przetwarzania danych osobowych w ramach prowadzonego postępowania oraz po zawarciu umowy:**

W ramach prowadzonego postępowania o udzielenie zamówienia publicznego realizowanego w formie zapytania ofertowego, będą przetwarzane dane osobowe zawarte w złożonych ofertach. Ponadto dane osobowe zawarte w wybranej ofercie będą przetwarzane dla potrzeb zawarcia umowy i jej dalszej realizacji. Wypełniając obowiązek prawny uregulowany zapisami art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019r. poz. 1781 t.j.), dalej jako „RODO", Biuro do spraw Substancji Chemicznych informuje, iż:

1) Administratorem Pani/Pana danych osobowych będzie Prezes Biura do spraw Substancji Chemicznych z siedzibą w Łodzi, ul. Dowborczyków 30/34;

2) Inspektorem Ochrony Danych (IOD) w Biurze do spraw Substancji Chemicznych jest Pan Krzysztof Domański. Skontaktować się z nim można poprzez e-mail: iod@chemikalia.gov.pl, lub pisemnie na adres siedziby administratora;

3) Dane osobowe będą przetwarzane w celu prawidłowego udzielenie zamówienia publicznego przez Biuro do spraw Substancji Chemicznych w Łodzi a w przypadku wyboru oferty dla potrzeb zawarcia umowy i jej dalszej realizacji; podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit b i c RODO;

4) Dane osobowe zawarte w ofercie mogą być udostępniane odbiorcom danych w rozumieniu art. 4 pkt.9 RODO, w szczególności w związku z realizacją obowiązku ustawowego w zakresie udzielenia informacji publicznej;

5) Dane osobowe mogą być przekazywane organom publicznym, organom ścigania lub innym organom ochrony prawnej (Policja, Prokuratura, Sąd) w związku z prowadzonym przez nie postępowaniem;

6) Dane osobowe nie będą przekazywane do państwa trzeciego ani do organizacji międzynarodowej;

7) Dane osobowe będą przetwarzane w zakresie niezbędnym do realizacji celu przetwarzania danych osobowych, nie dłużej niż przez okres wynikający z JRWA (jednolitego rzeczowego wykazu akt) obowiązującego u Biurze do spraw Substancji Chemicznych;

8) Przysługuje Panu/Pani prawo dostępu do treści swoich danych osobowych oraz ich sprostowania,

ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu wobec przetwarzania a także prawo do usunięcia danych jeżeli zaistnieją ku temu przesłanki;

9) Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

10) Podanie przez Pana/Panią danych osobowych jest niezbędne dla prawidłowego przeprowadzenia postępowania o udzielenie zamówienia publicznego. Niepodanie danych spowoduje, że nie będzie możliwe uwzględnienie w niniejszym postępowaniu złożonej oferty;

11) Pana/Pani dane osobowe nie będą podlegały zautomatyzowanym procesom podejmowania decyzji, w tym profilowaniu.

……

Anna Lewandowska

Dyrektor Generalny Biura do spraw Substancji Chemicznych

Łódź, 12.05.2022r.

/dokument podpisany elektronicznie/

W załączeniu:

1. Szczegółowy opis przedmiotu zamówienia.
2. Oświadczenie Wykonawcy o spełnianiu warunków.
3. Wzór druku dla propozycji cenowej.

Załącznik nr 1
do zaproszenia z dnia 12.05.2022 r.

PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest usługa hostingu dedykowanego wraz z łączem telekomunikacyjnym podłączonym do sieci Internet, odpowiednim oprogramowaniem systemowym oraz usługa serwisowa, konserwacyjna i administracyjna serwerów i firewall'a dla Biura do spraw Substancji Chemicznych.

Zamawiający określa poniżej szczegółowe warunki techniczne i specyfikacje przedmiotu zamówienia:

Minimalne wymagania techniczne dotyczące wynajmu serwerów oraz łącza telekomunikacyjnego na potrzeby stron internetowych Biura ds. Substancji Chemicznych

W ramach usługi hostingu dedykowanego Wykonawca udostępni Zamawiającemu dedykowane serwery podłączone, wraz z łączem telekomunikacyjnym do sieci Internet, wraz z odpowiednim oprogramowaniem systemowym. Wykonawca będzie świadczył również usługi serwisowe, konserwacyjne i administracyjne serwerów i firewall'a w okresie od dnia 1 czerwca 2022 r. do dnia 31 maja 2024 r w sposób ciągły, w systemie 24/7/365.

Hosting dedykowany przeznaczony jest do obsługi strony Krajowego Centrum Informacyjnego (clp.gov.pl i reach.gov.pl), serwisu www.eldiom.chemikalia.gov.pl prowadzonych przez Biuro ds. Substancji Chemicznych oraz strony www.chemikalia.gov.pl w formie archiwum (archiwum.chemikalia.gov.pl).

Wymogi niezbędne do realizacji zamówienia:

1. Wykonawca zapewni obsługę dowolnej liczby subdomen i baz danych, własne strony błędów, dostęp FTP do wydzielonego katalogu, a także przepisywanie adresu URL (mod-rewrite).
2. W ramach usługi hostingu dedykowanego, Wykonawca udostępni Zamawiającemu publiczne numery IP (w wersji IPv4 i IPv6 protokołu) w ilości potrzebnej do prawidłowego działania usługi hostingu (minimum 2).
3. Usługę hostingu dedykowanego Wykonawca będzie świadczył na umieszczonych w serwerowni dedykowanych serwerach podłączonych do Internetu, tj. serwera WWW działającego w modelu „passive-active" dla systemu Eldiom (opisanego w części „Parametry graniczne" L.p. I: 1-4 tabeli), serwera WWW dla pozostałych stron prowadzonych przez Biuro działającego w modelu „passive-active" (opisanych w części „Parametry graniczne" L.p. I: 5-8 tabeli), 1 sztuce serwera

(kopie zapasowe serwera www) - (opisanego w części „Parametry graniczne" L.p. II: 1-4 tabeli), 1 sztuce serwera Firewall (opisanego w części „Parametry graniczne" L.p. III: 1-4 tabeli).

4. Udostępnienie pomocniczego serwera nazw dla domen Biura ds. Susbtancji Chemicznych.
5. **Serwery, przy pomocy którego Wykonawca świadczył będzie usługę hostingową, umiejscowione będą na terytorium Rzeczypospolitej Polskiej.**
6. **Oprogramowanie systemowe:** Wykonawca na serwerach opisanych w części „Parametry graniczne" L.p. I: 1-4 tabeli) zainstaluje i skonfiguruje oprogramowanie systemowe (opisane w części „Parametry graniczne" L.p. IV: 1-10 tabeli),
    a. będzie wgrywał niezbędne aktualizacje do prawidłowego i niezawodnego działania oprogramowania systemowego.
    b. będzie sporządzał niezbędne kopie zapasowe nie rzadziej niż co 7 dni oraz nadzorował i administrował serwerami.
7. Parametry łącza (opisane w części „Parametry graniczne" L.p. V: 1-7 tabeli).
8. Zabezpieczenia fizyczne serwerowni (opisane w części „Parametry graniczne" L.p. VI: 1-13 tabeli).
9. Zasilanie i kontrola środowiska (opisane w części „Parametry graniczne" L.p. VII: 1-5 tabeli).
10. Bezpieczeństwo logiczne:

    Zawartości Serwisów WWW powinna być chroniona przed niepożądanym dostępem polegającym na niedopuszczeniu do modyfikacji Serwisów WWW przez nieuprawnionych użytkowników, a jeżeli takie zjawisko nastąpi, na dokładnym monitorowaniu i udaremnieniu takiej próby.

    Całe centrum przetwarzania danych Wykonawcy powinno być zabezpieczone redundantnym systemem ścian ogniowych (firewall). Firewalle muszą kontrolować cały ruch wchodzący i wychodzący z Centrum, przepuszczając wyłącznie pakiety niezbędne dla prawidłowego działania serwisów. Blokować adresy IP powodujących największe obciążenie Serwisów WWW w danej jednostce czasu.

    Dodatkowo Zamawiający wymaga własnego Firewalla o konfiguracji opisanej w części „Parametry graniczne" L.p. III: 1-3 tabeli na którym będą konfigurowane reguły tylko dla serwerów zamawiającego. Administrowanie wszystkimi serwerami powinno odbywać się zdalnie z siedziby Wykonawcy poprzez bezpieczne szyfrowane połączenie.

    Anty DDoS - usługa musi pozwalać na skuteczne identyfikowanie oraz izolowanie podejrzanego ruchu w zakresie ataków typu DDoS. (np. sinkholing) Usługa musi być świadczona w dwóch warstwach dostępowych:

    a. warstwa pierwsza – operator telekomunikacyjny – Wykonawca musi posiadać stosowne umowy z operatorami telekomunikacyjnymi w celu ochrony własnej sieci przed atakami wolumetrycznymi o bardzo dużym nasileniu mogącymi w skrajnym przypadku wysycić

w całości łącze operatora. W takim przypadku ochrona jest realizowana w warstwie operatora.
b. warstwa druga – Wykonawca musi posiadać własne rozwiązanie przed atakami DDoS dzięki czemu jest wstanie w całości zarządzać konfiguracją filtrów i poziomów ochrony. Zastosowane rozwiązanie musi spełniać funkcję drugiej warstwy ochrony operującą w ramach ataków wolumetrycznych w warstwie 3 i 4 modelu IOS/OSI.

11. **Kopie bezpieczeństwa** (opisana w części „Parametry graniczne" L.p. VIII: 1-2 tabeli)
12. **Gwarancja jakości (SLA)**

- Gwarantowana dostępność serwera, usług oraz łącza 99,9% w skali miesiąca. Gwarancja dostępności definiowana jest poprzez stosunek ilości czasu w którym serwer jest dostępny w ciągu miesiąca (w minutach) do całkowitej ilości czasu w ciągu miesiąca (w minutach). Do czasu braku dostępności nie wchodzą uzgodnione przerwy serwisowe oraz wszystkie inne zaakceptowane przez Zamawiającego.
- Wykonawca dołoży wszelkich starań by zapewnić nienaruszalność i integralność danych przechowywanych na serwerze. W razie naruszenia bezpieczeństwa serwerów Wykonawca niezwłocznie poinformuje o tym Zamawiającego oraz przywróci dane z ostatniej kopii zapasowej do stanu sprzed zdarzenia.

13. **Planowany przebieg i zakres prac**

Zakres prac Wykonawcy obejmuje prace wdrożeniowo-instalacyjne wykonywane jednokrotnie przed uruchomieniem systemu oraz prace administracyjne wykonywane rutynowo przez cały czas świadczenia usług.

14. **Działania jednorazowe do wykonania nie później niż do dnia 1 czerwca 2022 r.**

- Przeniesienie danych z obecnych serwerów Biura na serwery Wykonawcy.
- Uruchomienie systemów i stron Biura na serwerach Wykonawcy.
- Uzgodnienie szczegółowych wymagań instalacyjnych i konfiguracyjnych z Zamawiającym
- Opracowanie procedur sporządzania backupów.
- Dostawa sprzętu zgodnie ze specyfikacją.
- Instalacja urządzeń.
- Instalacja oprogramowania systemowego.
- Konfiguracja sprzętu i oprogramowania systemowego zgodnie z wymaganiami Zamawiającego.

15. **Działania rutynowe**

- Monitoring działania systemu.
- Wykonywanie kopii zapasowych zgodnie z procedurą zawartą w części „Parametry graniczne" L.p. VIII: 1-2 tabeli.
- Nadzór administracyjny systemu.

- Aktualizacja wersji oprogramowania systemowego w razie wykrycia w nim błędów bezpieczeństwa.

16. **Okienko serwisowe**

Działania serwisowe wymagające zatrzymania działania serwisów (np. instalacje nowych wersji sprzętu i oprogramowania) prowadzone będą w ramach okienek serwisowych, kiedy działanie serwisu nie jest niezbędne. Zamawiający będzie informowany o planowanych przerwach z 24 godzinnym wyprzedzeniem. Prace serwisowe prowadzone w ramach zaplanowanych okienek nie będą zaliczane do czasu awarii serwera przy liczeniu współczynnika dostępności.

17. **Wymagania dla serwisów internetowych w domenie gov.pl**

Ponadto wykonawca zapewni spełnienie wymagań dla serwisów internetowych w domenie gov.pl zawartych w części 2 „Wymagania dla serwisów internetowych w domenie gov.pl" w zakresie dostępności i integralności dla serwisu klasy 4 dla eldiom.chemikalia.gov.pl oraz 2 dla clp.gov.pl i reach.gov.pl

18. Zapewnienie ochrony stron odpowiednimi certyfikatami (eldiom.chemikalia.gov.pl, archiwum.chemikalia.gov.pl - Certyfikaty Organization Validated (OV) zapewniają potwierdzenie tożsamości oraz silną ochronę SSL, natomiast strony clp.gov.pl i reach.gov.pl - Certyfikaty Domain Validation (DV)).

1. PARAMETRY GRANICZNE:

L.p.	Parametr	Wymagania minimalne
I.	**Serwery WWW działające w modelu PASSIVE-ACTIVE.**	
	Serwer WWW dla systemu ELDIOM	
1.	Procesor	Minimum dwie sztuki procesorów czterordzeniowych o wydajności co najmniej 12000 punktów w rankingu cpubenchmark.net (CPU Lis High End CPUs),
2.	Pamięć RAM	Minimum 64 GB
3.	Dysk twardy	Minimum 2 TB powierzchni użytkowej dostępnej lokalnie na serwerze
4.	Napęd	DVD –RW
	Serwer WWW	
5.	Procesor	Minimum dwie sztuki procesorów czterordzeniowych o wydajności co najmniej 7000 punktów w rankingu cpubenchmark.net (High End CPUs),

6.	Pamięć RAM	Minimum 12 GB
7.	Dysk twardy	Minimum 500 GB powierzchni użytkowej dostępnej lokalnie na serwerze
8.	Napęd	DVD –RW

II.	**1 sztuka serwera (kopia zapasowa serwera www)**	
1.	Procesor	Minimum procesor czterordzeniowy o wydajności co najmniej 10000 punktów w rankingu cpubenchmark.net (High End CPUs)
2.	Pamięć RAM	Minimum 8 GB
3.	Dysk twardy	Minimum 1 TB powierzchni użytkowej dostępnej lokalnie na serwerze.
4.	Napęd	DVD –RW
III.	**1 sztuka serwera Firewall lub dedykowanego Firewall'a przeznaczonego do kontrolowania ruchu pakietów kierowanych do serwerów stron Biura, umożliwiającego tworzenie reguł bezpieczeństwa, blokowanie ataków np. DoS, DDoS, skanowanie portów, zarządzanie ruchem skierowanym poprzez FTP do serwera, o parametrach nie mniejszych niż podane w pkt. III: podpunkty 1-4 tabeli**	
1.	Funkcje Firewall	• Działająca funkcja IPS obsługująca w czasie rzeczywistym zagrożenia typu nadużycie protokołu, próby tunelowania, oprogramowania typu exploit, kontrola aplikacji, ataki ogólnego typu bez predefiniowanych sygnatur, ruchu generowanego przez szkodliwe oprogramowanie, podatności serwera i klienta wraz z możliwością definiowania własnych sygnatur. • Rozwiązanie musi być wyposażone w gotowe reguły filtracyjne (aktualizowane codziennie) umożliwiające ochronę przez znanymi zagrożeniami, w ramach których można wymienić: SQL Injection (SQLi), Cross Site Scripting (XSS), Local File Inclusion (LFI), Remote File Inclusion (RFI), Remote Code Execution (RCE), PHP Code Injection, HTTP Protocol Violations, HTTPoxy, Shellshock, Session Fixation, Scanner Detection, Metadata/Error Leakages19, Project Honey Pot Blacklist, GeoIP Country Blocking, Directory Traversal. • Rozwiązanie musi umożliwiać tworzenie własnych reguł. • Rozwiązanie musi wspierać mechanizmy bezpieczeństwa uwzględniające: · reputację IP · wykrywanie złośliwego oprogramowania na bazie ruchu Web · wykrywanie złośliwego oprogramowania typu backdoor · wykrywanie ataków typu Botnet · wykrywanie ataków typu HTTP Denial of Service (DoS) · Anti-Virus w zakresie plików Możliwość zestawienia VPN'a,
IV.	**Oprogramowanie systemowe**	
	Serwer WWW dla systemu ELDIOM	
1.	System operacyjny	Windows Server 2012 R2 lub nowszy
2.	Oprogramowanie	MS SQL 2008 R2 lub nowszy JBOSS 5.1.0.GA
	Serwer WWW	
3.	System operacyjny	Linux - preferowany Centos 6.x lub równoważny system operacyjny, tzn. umożliwiający poprawną współpracę z systemami CMS zamawiającego

4.		MySQL 5.1 .x pracujący w systemie replikacji typu master-master na obu serwerach WWW
5.		nginx w wersji 0.7.x, 1 .x, bądź Apache w wersji 2.2.x lub nowszych
6.		OpenSSL 1.0.1g lub nowsze
7.		phpMyAdmin min 5.3.x lub nowszy
8.	Oprogramowanie	Cache pamięciowy: memcached
9.		ModSSL 2.8.25 lub nowszy
10.		Interpreter skryptów PHP w wersji min 5.3.x z zainstalowanymi modułami: +IonCube +bz2 +curl +gd
V.	**Parametry łącza**	
1.	transfer danych	Bez limitu ilości przesyłanych danych podczas okresu trwania umowy
2.	Gwarantowana przepustowość (CIR) w Serwerowni	1 Gbps Połączenia realizowane przez co najmniej 2 różnych operatorów telekomunikacyjnych.
3.	Firewall operatora	Łącze w Serwerowni chronione niezależnym systemem Firewall z IPS online z korelacją zdarzeń i usługami oceny zagrożeń
VI.	**Zabezpieczenia fizyczne serwerów Wykonawcy**	
1.	Serwerownia	Wykonawca oświadczy, iż serwerownia znajduje się w profesjonalnie, całodobowo chronionym przez licencjonowaną firmę ochrony osób i mienia budynku,
2.		Dostęp do serwerowni musi wymagać autoryzacji pracownika
3.		Serwerownia ma być wyposażona w system alarmowy oraz monitoring telewizji przemysłowej
4.		Wszystkie serwery muszą być umieszczone w zamykanych na klucz szafach przemysłowych
5.		Serwerownia musi posiadać system zabezpieczeń przeciwpożarowych
6.		Energia elektryczna ma być dostarczana z dwóch niezależnych przyłączy energetycznych, a wszystkie urządzenia na których będzie świadczona usługa muszą być podpięte do centralnego systemu podtrzymywania napięcia.
7.		Serwerownia musi dysponować własnym systemem bezawaryjnego zasilania (w tym m.in. agregat prądotwórczy z zapasem paliwa na co najmniej 12h ciągłej pracy przy obciążeniu 75% z możliwością dotankowania agregatu bez przerwy w działaniu).
8.		Nadzór 24h operatora znajdującego się na terenie Serwerowni z czasem reakcji na awarię 15 minut.
VII.	**Zasilanie i kontrola środowiska**	
1.	Zasilanie	Wszystkie urządzenia muszą być podpięte do centralnego systemu podtrzymywania napięcia.
2.		Serwerownia musi dysponować własnym systemem bezawaryjnego zasilania.
3.	Przeciwdziałanie awariom	Serwery powinny być wyposażone w system wczesnego wykrywani awarii monitorujący dyski twarde, wentylatory, zasilacze, pamięć, procesory, moduły regulacji napięcia, przewidujący możliwość wystąpienia awarii danego elementu przed jej faktycznym wystąpieniem.
VIII.	**Kopie bezpieczeństwa**	

1.	Bezpieczeństwo danych	Na serwerze do backup-ów - backup ma być prowadzony w trybie: • w cyklu codziennym: - ELDIOM - backup przyrostowy systemu plików i bazy danych (MSSQL) w trybie ciągłym co 12 godzin, - - WWW - backup przyrostowy systemu plików i bazy danych (mysql) w trybie ciągłym co 24 godzin, • w cyklu tygodniowy - backup pełny. Zamawiający wymaga posiadania kopii zapasowej pozwalającej na powrót do stanu sprzed 24 godzin. Zamawiający wymaga by system wykonywania kopii zapasowych umożliwiał całościowe i selektywne odzyskiwanie danych, zarówno w zakresie całych maszyn wirtualnych, jak i poszczególnych plików w ramach maszyn wirtualnych.
2.		Dodatkowo kopie zapasowe mają być tworzone automatycznie na zewnętrznej macierzy dyskowej o przestrzeni nie mniejszej niż 1 TB, znajdującej się w niezależnej geograficznie lokalizacji - Serwerowni Zapasowej.
IX. Inne		
1. Udostępnienie infolinii umożliwiającej zgłaszanie i rejestrowanie problemów oraz połączenie z konsultantem w kwestiach związanych z eksploatacją systemu 2. Udostępnienie wykonawcy systemu możliwości zdalnego dostępu do zasobów systemowych na poziomie administratora 24/7/365 w celu weryfikacji, naprawy lub prac serwisowych 3. SLA na poziomie minimum 99,9%.		

2. Wymagania dla serwisów internetowych w domenie gov.pl

Poniżej zamieszczono wymagania dla serwisów internetowych w domenie gov.pl opracowane przez Ministerstwo Administracji i Cyfryzacji. Ich stosowanie jest wymagane w przypadku stron internetowych urzędów znajdujących się w domenie gov.pl.

	Wymagania dla serwisów internetowych w domenie GOV.PL			Klasa serwisu / witryny 1	2	3	4	5	6	7	8
DOSTĘPNOŚĆ	Redundancja	Łącze	Active-Active	-	-	O	O	X	X		
			Passive-Active	O	O	X	X	-	-		
		Zasilanie	Active-Active	-	-	O	O	X	X		
			Passive-Active	O	O	X	X	-	-		
		Sprzęt	Active-Active	-	-	O	O	X	X		
			Passive-Active	O	O	X	X	-	-		
	Skalowalność	Łącze		O	O	O	O	X	X		
		Wydajność	Sprzęt	-	O	O	O	O	X		
			Wirtualizacja	O	-	X	X	X	X		
	Wdrożenie rozwiązań rozproszonych w trybie on-demand		Chmura	-	O	O	O	O	X		
			Rev-proxy + round-robin	-	-	-	O	O	X		
	Serwowanie wersji dynamicznej (frontend+baza danych)/wersji statycznej (czysty html) w zależności od obciążenia systemu i łącza			-	O	O	X	X	X		
	Centrum zapasowe		offline	O	O	X	X	-	-		
			online	-	-	O	-	X	X		
INTEGRALNOŚĆ	Okresowa (częsta) weryfikacja zapisów treści (sumy kontrolne)			X	X	X	X	X	X		
	Odpowiednia konfiguracja praw dostępu serwisu serwera WWW		tylko odczyt (wersja statyczna)	X	-	X	X	X	X		
			minimalne prawa dostępu do baz (wersja dynamiczna)	-	X	X	X	X	X		
	uwierzytelnianie dokumentów krytycznych dla obywatela			-	-	X	X	X	X		
	Brzegowe rozwiązania bezpieczeństwa (IPS/IDS/AV/FW)			X	X	X	X	X	X		
	Strefowanie systemu z zachowaniem minimalnych praw			-	O	X	X	X	X		
	Wewnętrzne rozwiązania bezpieczeństwa (IPS/IDS/AV/FW)			O	X	X	X	X	X		
	Wdrożenie sondy ARAKIS-GOV			O	X	X	X	X	X		
	Kontrola integralności serwisu na potrzeby użytkownika poprzez możliwość przełączenia połączenia na https weryfikowalne przy pomocy certyfikatu umiejscowionego w drzewie akredytowanym przez przeglądarkę			O	X	X	X	X	X		
POUFNOŚĆ	Połączenie szyfrowane		logowanie użytkowników uprzywilejowanych	X	X	X	X	X	X		
			logowanie użytkowników zewnętrznych	-	-	-	-	X	X		
			przesyłanie informacji przez uż. zewnętrznych	-	-	-	-	X	X		
	Przechowywanie danych w formie zaszyfrowanej		dane do logowania	X	X	X	X	X	X		
			informacje od uż. zewnętrznych	-	-	-	-	X	X		
	Konta użytkowników zarządzających treścią		tylko dla pracowników jednostki	X	X	X	X	X	X		
			dostępne tylko z określonych adresów IP	O	X	X	X	X	X		

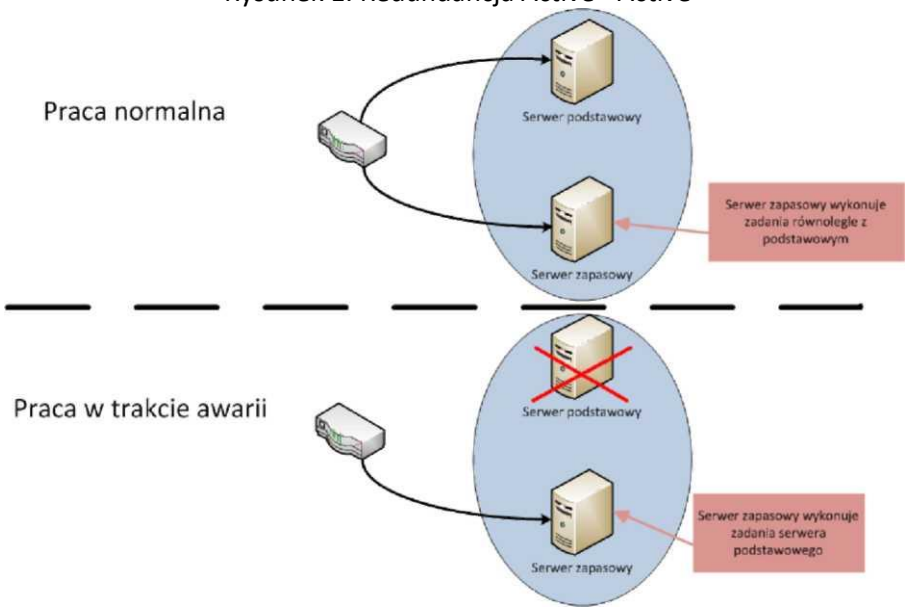
1	prosta publikacja informacji o jednostce
2	dynamiczna, informacyjna strona www
3	BIP
4	strona zawierająca informacja dla obywateli stanowiące podstawę ich dalszych działań (np. formularze)
5	strona zawierająca dynamiczne formularze, które po wypełnieniu stanowią podstawę działań po stronie jednostki
6	strona zawierająca dwustronny system wymiany informacji jednostka <-> obywatel

O Opcjonalne
X Zalecane
- Nie dotyczy

Wyjaśnienie użytych pojęć:

1. Anti-virus (AV) – oprogramowanie mające na celu wykrywanie złośliwego oprogramowania przekazywanego przez różne media (np. sieć komputerową, dyski, pen-drive), które może zakłócić działanie systemu lub umożliwić włamanie do niego. ARAKIS-GOV (sonda) – patrz Sonda ARAKIS-GOV.
2. Centrum zapasowe – infrastruktura informatyczna obejmująca sprzęt komputerowy, łącza, sieć energetyczną itp. Umożliwiająca awaryjne uruchomienie wszelkich usług działających w centrum głównym; centrum zapasowe może działać w trybie offline – włączane tylko w przypadku awarii centrum głównego oraz w trybie online – jest włączone cały czas, ale wykorzystuje się jego zasoby dopiero w momencie awarii; dopuszcza się mniejszą wydajność centrum zapasowego oraz możliwość utraty integralności danych w czasie uruchamiania centrum zapasowego.
3. Chmura (ang. Cloud) – usługa świadczona najczęściej przez zewnętrznych dostawców udostępniająca zasoby umożliwiające uruchomienia własnych usług lub aplikacji; udostępnione zasoby mogą stanowić środowisko rozproszone (np. serwery usługowe mogą znajdować się w rozproszonych lokalizacjach); zasoby te należą do dostawcy i mogą być wynajmowane na określonych warunkach (np. dzierżawa); zasoby mogą stanowić zarówno infrastrukturę (sprzęt), jak i oprogramowanie (np. serwery WWW, oprogramowanie biurowe); termin chmura jest bardzo ściśle związany z pojęciem wirtualizacji.
4. CMS (ang. Content Management System, pol. System Zarządzania Treścią) – oprogramowanie osadzone na serwerze WWW pozwalające na łatwe utworzenie serwisu WWW oraz jego późniejszą aktualizację i rozbudowę oraz zarządzanie treścią (publikowaną informacją).
5. Dane zaszyfrowane – dane przechowywane najczęściej w bazie danych w postaci uniemożliwiającej ich odczytanie w sposób nieautoryzowany przez osoby nieupoważnione.
6. Firewall (FW) (pol. ściana ogniowa) – rozwiązanie sprzętowe lub oprogramowanie umożliwiające filtrowanie ruchu sieciowego do i z wydzielonego systemu komputerowego (komputer, sieć prywatna) mające na celu ochronę przed niepowołanym dostępem do chronionego systemu, jak i ochronę przed wypływem danych z tego systemu; najczęściej występuje w postaci dedykowanego serwera z zainstalowanym specjalistycznym oprogramowaniem.
7. IPS, IDS (ang. Intrusion Prevention System – pol. System Zapobiegania Włamaniom, Intrusion Detection System – pol. System Wykrywania Włamań) – urządzenie sieciowe zwiększające bezpieczeństwo sieci komputerowych poprzez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym; wykorzystuje zaawansowane metody analizy heurystycznej i sygnaturowej ruchu sieciowego.
8. Połączenie szyfrowane – połączenie sieciowe, w którym przesyłane informacje szyfrowane są za pomocą określonego algorytmu uniemożliwiającego podsłuchiwanie treści przez osoby nieupoważnione (do informacji mają dostęp tylko nadawca i adresaci).
9. Redundacja – zastosowanie nadmiarowych zasobów (np. serwerów, łącza) w celu zabezpieczenia systemu przed przerwą w działaniu, na wypadek uszkodzenia zasobów podstawowych (np. dodatkowe serwery, dodatkowe łącze internetowe itp.).
10. Redundacja w trybie Active – Active – typ nadmiarowego wykorzystania zasobów, w której zasoby zapasowe (np. serwery) są cały czas aktywne (włączone) i wykonują swoją celową pracę równocześnie z zasobami głównymi.

Rysunek 1. Redundancja Active - Active

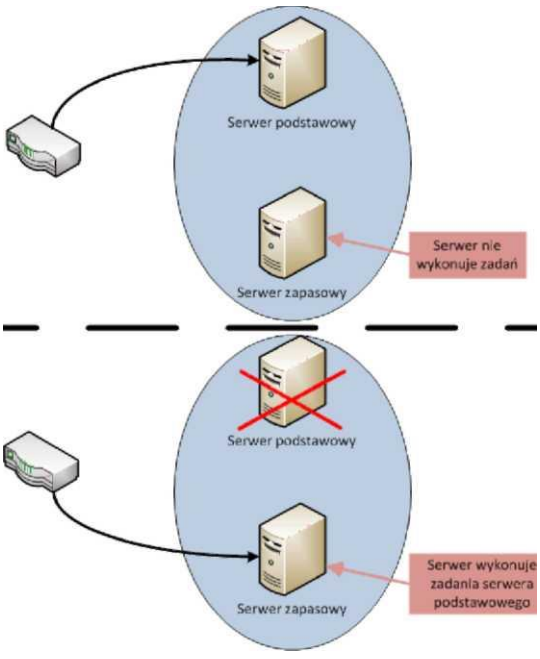


11. Redundacja w trybie Passive – Active – typ nadmiarowego wykorzystania zasobów, w której zasoby zapasowe są wyłączone (pasywne) w czasie prawidłowego działania systemu, a włączają się (stają się Aktywne) w razie awarii zasobów głównych.

Rysunek 2. Redundancja Passive - Active

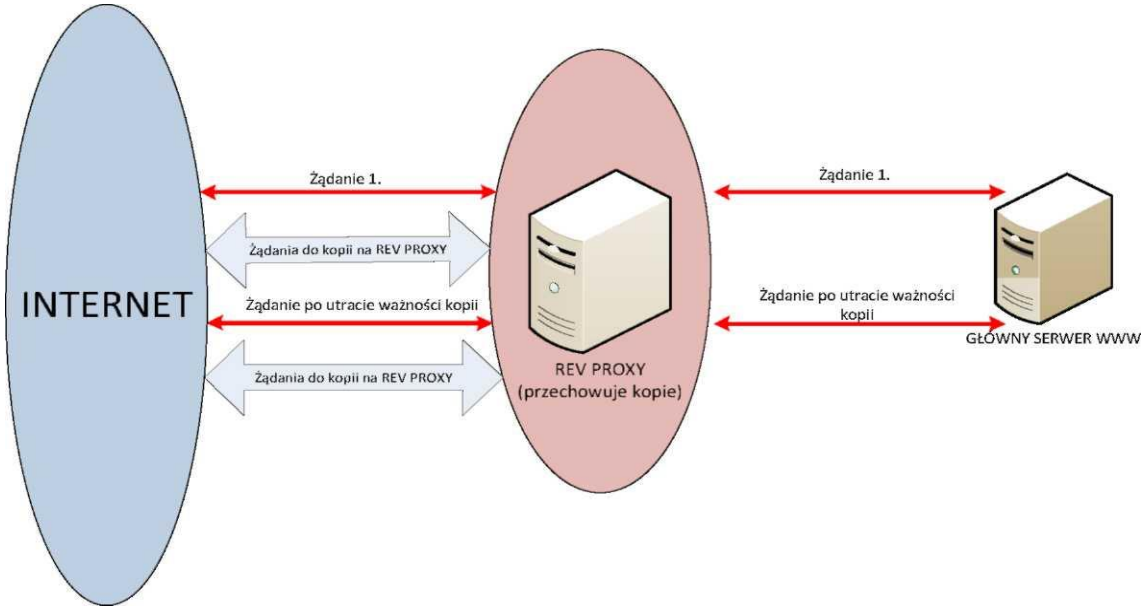
PRACA NORMALNA

PRACA W TRAKCIE AWARII



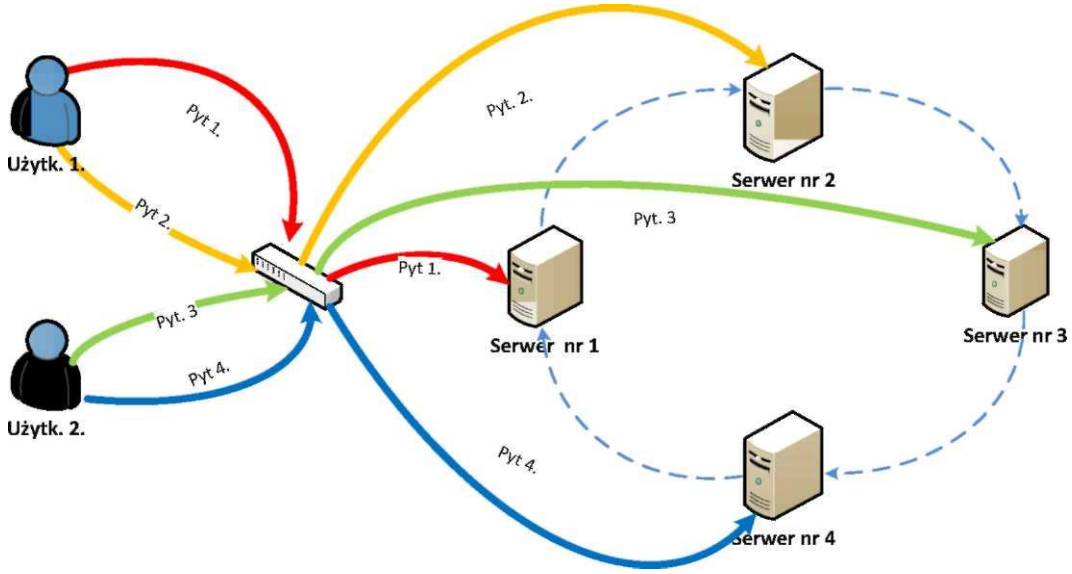
12. Rev-Proxy - specjalny rodzaj serwera Proxy umożliwiający zmniejszenie obciążenia głównego serwera WWW i przyspieszenie ładowania serwowanej witryny; serwer rev-proxy wykonuje lokalne kopie elementów strony WWW żądanych przez klienta; każde następne żądanie tego elementu będzie obsługiwane przez serwer rev-proxy, a nie przez serwer WWW do czasu, aż ten element strony straci ważność (np. z powodu upływu czasu ważności lub zmiany elementu).

Rysunek 3. Działanie Rev - Proxy



13. Rev – Proxy + round – robin – przy większej niż 1 liczbie serwerów Rev – Proxy możliwe jest zastosowanie techniki balansowania ruchu (load – balancing), np. w technice round-robin, polegającej na rozkładaniu ruchu na różne serwery rev-proxy, gdzie każde kolejne żądanie przekazywane jest w pętli do kolejnych serwerów:
    - żądanie 1. -> serwer 1.
    - żądanie 2. -> serwer 2.
    - żądanie 3. -> serwer 3.
    - żądanie 4. -> serwer 4.
    - żądanie 5. -> serwer 1.
    - żądanie 6. -> serwer 2.
    - żądanie 7. -> serwer 3.
    - żądanie 8. -> serwer 4.

Rysunek 4. Działanie algorytmu Round – Robin.



14. Serwis dynamiczny - serwis WWW, którego działanie opiera się na jego dynamicznym wygenerowaniu po stronie serwera i przesłaniu do przeglądarki klienta jako strony HTML; najczęściej serwisy dynamiczne opierają się na wykorzystaniu systemu zarządzania treścią (CMS), który komunikując się z bazą danych pobiera dane do wyświetlenia, a następnie generuje stronę WWW; wymaga większych zasobów niż serwis statyczny, trudniejszy w skalowaniu, jest bardziej podatny na zagrożenia ze względu na większy stopień skomplikowania, daje większe możliwości rozbudowy treści witryn.
15. Serwis statyczny - serwis WWW zbudowany o czysty HTML bez dynamicznego generowania treści oraz wyglądu; wymaga mniejszych zasobów niż serwis generowany dynamicznie, łatwiejszy w skalowaniu, łatwiejszy w utrzymaniu bezpieczeństwa, nie daje możliwości łatwej rozbudowy treści.
16. Skalowalność - zdolność danego systemu do przystosowywania się do coraz większego obciążenia, np. w przypadku zwiększania oglądalności witryny system je udostępniający powinien być coraz wydajniejszy; zdolność przystosowania można rozumieć jako łatwość rozbudowy o nowe elementy w zależności od potrzeb, np.: większa liczba odsłon witryny powinna automatycznie uruchomić dodatkowe serwery obsługujące te żądania.
17. Sonda ARAKIS-GOV - urządzenie podłączane w infrastrukturze udostępniającej stronę WWW monitorujące ruch sieciowy skierowany do tej witryny w celu wykrywania anomalii sieciowych, które mogą być źródłem potencjalnego ataku; pozwala na automatyczną obserwację potencjalnych zagrożeń (robaków, wirusów, skanów) usiłujących przedostać się do wykorzystywanej infrastruktury.
18. Strefowanie systemu z zachowaniem minimalnych praw - przydzielanie minimalnych uprawnień użytkownikom wymaganych do działania w poszczególnych elementach systemu informatycznego (strefie); np.: strefa administracyjna - prawa odczytu danych, tworzenia użytkowników, itp., strefa publiczna - tylko odczyt danych.
19. Sumy kontrolne - mechanizm weryfikacji treści polegający na wyliczeniu specjalnym algorytmem (np. MD5, SHA1) ciągu znaków (np. liczby) unikalnego tylko dla tej treści; dwa

takie same teksty powinny mieć taką samą sumę kontrolną, pozwala to wykryć np. nieautoryzowane zmiany w treściach umieszczanych na witrynie WWW.

20. Użytkownik zarządzający treścią - użytkownik serwisu opartego na systemie zarządzania treścią (CMS) mający uprawnienia do tworzenia, modyfikowania i kasowania treści udostępnianych przez ten system.
21. Wirtualizacja - uruchomienie na wysoko - wydajnym systemie komputerowym (tzw. Host - system Gospodarz) wielu systemów operacyjnych (tzw. Guest - system Gość) tak, że ma on wrażenie, że działa na wydzielonym sprzęcie; technika ta ma na celu efektywniejsze wykorzystanie zasobów sprzętowych oraz w wielu przypadkach zmniejszenie kosztów rozbudowy infrastruktury informatycznej, np. uruchomienie na jednym wydajnym serwerze wielu serwerów baz danych oraz serwerów WWW do obsługi witryny internetowej.

Załącznik nr 2
do zaproszenia z dnia 12.05.2022 r.

OŚWIADCZENIE

Firma(nazwa) Wykonawcy:

……..

Osoba (-y) upoważniona (-e) do reprezentowania Wykonawcy:

……

……..

Adres Wykonawcy:

……

……

Oświadczam niniejszym, że:

1. Jestem uprawniony do występowania w obrocie prawnym, zgodnie z wymogami ustawowymi.
2. Posiadam niezbędną wiedzę i doświadczenie oraz potencjał techniczny, a także dysponuję osobami zdolnymi do wykonania zadania.
3. Znajduję się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zadania.

Podpisano:

…… .....

Osoba (-y) upoważniona (-e) do reprezentacji Wykonawcy miejscowość i data

Załącznik nr 3

do zaproszenia z dnia 12.05.2022 r.

PROPOZYCJA CENOWA

Odpowiadając na zaproszenie do złożenia propozycji cenowej na zadanie dotyczące usługi hostingu dedykowanego wraz z łączem telekomunikacyjnym podłączonym do sieci Internet, odpowiednim oprogramowaniem systemowym oraz usługą serwisową, konserwacyjną i administracyjną serwerów i firewall'a dla Biura do spraw Substancji Chemicznych:

1. Oferuję wykonanie usługi będącej przedmiotem zamówienia, zgodnie z wymaganiami opisu przedmiotu zamówienia:

    1) Cena usługi brutto (za jeden miesiąc) – ……
    2) Całkowita cena usługi brutto za cały okres realizacji usługi - ……

Na ww. cenę brutto składają się opłaty za poszczególne usługi:

……

……

……

2. Wymagany termin realizacji zamówienia: od 01.06.2022 r. do 31.05.2024 r.

3. Załącznikami do propozycji są: dokumenty i załączniki wymienione w ust. 5 zaproszenia.

……

(data, podpis Wykonawcy)