MAZOWIECKI
URZĄD WOJEWÓDZKI
W WARSZAWIE

Mazowiecki Urząd Wojewódzki w Warszawie
Pl. Bankowy 3/5
00-950 Warszawa

OPIS PRZEDMIOTU ZAMÓWIENIA

świadczenie usługi hostingu

Spis treści

I. Definicje

1. **Błąd** – Błąd krytyczny, Błąd niekrytyczny.
2. **Błąd krytyczny** – Błąd krytyczny Środowiska Produkcyjnego, Błąd krytyczny Środowiska Testowego, Błąd krytyczny Środowiska Szkoleniowego.
3. **Błąd krytyczny Środowiska Produkcyjnego** – błąd Środowiska Produkcyjnego uniemożliwiający dostęp do wszystkich funkcjonalności Platformy, traktowany jako niedostępność i rozliczany zgodnie z wymaganiami SLA.
4. **Błąd krytyczny Środowiska Testowego** – błąd Środowiska Testowego uniemożliwiający dostęp do wszystkich funkcjonalności Platformy, traktowany jako niedostępność i rozliczany zgodnie z wymaganiami SLA.
5. **Błąd krytyczny Środowiska Szkoleniowego** – błąd Środowiska Szkoleniowego uniemożliwiający dostęp do wszystkich funkcjonalności Platformy, traktowany jako niedostępność i rozliczany zgodnie z wymaganiami SLA.
6. **Błąd niekrytyczny**– każda inna awaria niebędąca Błędem krytycznym.
7. **CPD** – Centrum Przetwarzania Danych – zasoby informatyczne Zamawiającego.
8. **Czas usunięcia Incydentu** – czas liczony od momentu zgłoszenia Incydentu przez Zamawiającego w systemie zgłoszeniowym Wykonawcy, do momentu przywrócenia wszystkich funkcjonalności Środowiska.
9. **EOG** - Europejski Obszar Gospodarczy (*ang. European Economic Area, EEA*).
10. **Incydent** – oznacza nieprawidłowość w dostępności usługi hostingu i/lub awarii dla Środowisk.
11. **Okres rozliczeniowy** – okres realizacji przedmiotu Umowy przez Wykonawcę podlegający raportowaniu i rozliczaniu. Okres rozliczeniowy obejmuje pełny miesiąc kalendarzowy, w przypadku podpisania umowy w pierwszym dniu miesiąca. W przypadku podpisania umowy w innym dniu, Okres rozliczeniowy obejmuje okres trwający 30/31 dni od daty wynikającej z dnia podpisania umowy (np. od 21 dnia danego miesiąca do 20 następnego miesiąca).
12. **OPZ** – Opis Przedmiotu Zamówienia.
13. **Platforma** – system teleinformatyczny Zamawiającego, mający na celu udostępnienie i zarządzanie wysokiej jakości usługami publicznymi, świadczonymi drogą elektroniczną przez Zamawiającego, zintegrowany z systemami EZD, ePUAP, Profil Zaufany.
14. **Przerwa techniczna** – przerwa w dostępie do usługi hostingu, spowodowana prowadzeniem planowanych prac konserwacyjnych. Przerwa wliczana jest do czasu niedostępności w Okresie rozliczeniowym.
15. **Raport okresowy** - raport który będzie przedstawiał wyniki osiągnięte w danym Okresie rozliczeniowym.
16. **Środowisko** - Środowisko Produkcyjne, Środowisko Testowe, Środowisko Szkoleniowe.
17. **Środowisko produkcyjne** - środowisko, na którym skonfigurowana będzie finalna wersja Platformy, gotowa do udostępnienia użytkownikom.
18. **Środowisko szkoleniowe** - środowisko, na którym udostępniona będzie finalna wersja Platformy dla celów szkoleń.
19. **Środowisko testowe** - środowisko, na którym będą testowane kolejne wersje Platformy i funkcjonalności gotowe w postaci prototypów do weryfikacji dla Zamawiającego.
20. **Umowa –** Umowa zawarta między Zamawiającym z Wykonawcą na świadczenie usługi hostingu.
21. **Wykonawca** – podmiot wybrany w wyniku postępowania przetargowego.
22. **Zamawiający** - Mazowiecki Urząd Wojewódzki w Warszawie (MUW).

I. Przedmiot zamówienia

1. Przedmiotem zamówienia jest świadczenie usługi hostingu Środowisk dla Platformy zgodnie z parametrami określonymi w niniejszym OPZ.
2. Wykonawca w ramach świadczenia usługi hostingu na podstawie Umowy, uruchomi i będzie utrzymywał, co najmniej następujące niezależne Środowiska:
    a. Środowisko produkcyjne,
    b. Środowisko testowe,
    c. Środowisko szkoleniowe .
3. Usługa ma być świadczona w oparciu o dedykowane maszyny wirtualne.
4. W ramach realizacji usługi, Wykonawca musi zapewnić:
    a. łącze do sieci Internet oraz umożliwić zestawienie połączenia VPN typu site-site z Centrum Przetwarzania Danych (CPD) Zamawiającego;
    b. infrastrukturę teletechniczną wraz z niezbędnymi urządzeniami, oprogramowaniem i licencjami niezbędnymi do uruchomienia i prawidłowego działania usług zgodnie z parametrami określonymi w niniejszym OPZ;
    c. obsługę infrastruktury umożliwiającej działanie Środowisk dla Platformy;
    d. wykonywanie kopii bezpieczeństwa wszystkich serwerów i bazy danych;
    e. ochronę antywirusową, ochronę przed atakami i infekcją złośliwego oprogramowania.

II. Wymagania szczegółowe

W ramach realizacji przedmiotu zamówienia do zadań Wykonawcy będzie należało w szczególności:

1. Zapewnienie maszynom wirtualnym wysokiej dostępności oraz wysokiej niezawodności działania platformy sprzętowo-systemowej poprzez umożliwienie działania Platformy w architekturze High Availability, zapewniającej dostępność na poziomie 99,7% w każdym okresie rozliczeniowym.

2. Zapewnienie skalowalności Środowisk poprzez możliwość zwiększenia liczby serwerów oraz rozbudowy serwerów w celu zwiększenia ich mocy obliczeniowej.

3. Zapewnienie poufności, integralności, bezstratności danych, w tym danych pozyskanych i przetworzonych z sieci Internet.

4. Odseparowanie Środowiska produkcyjnego od testowego i szkoleniowego na poziomie platformy systemowej, w taki sposób, aby awaria jednego z nich nie miała wpływu na inne, a przede wszystkim Środowisko produkcyjne.

5. Nie nakładanie odgórnych blokad ruchu z/do środowiska hostingowego w ramach dedykowanych maszyn wirtualnych (dotyczy zakresów IP, podsieci, portów) bez uzasadnionej przyczyny.

6. Zapewnienie przepustowości połączeń sieciowych między komponentami w ośrodku przetwarzania danych na poziomie nie mniej niż 10 Gbps, z zachowaniem redundancji połączeń;

7. Zapewnienie przepustowości pomiędzy serwerami, a zasobami dyskowymi na poziomie nie mniej niż 8 Gbps z zachowaniem redundancji połączeń.

8. Zapewnienie przepustowości symetrycznego łącza dostępowego do sieci Internet (CIR/EIR) nie mniejszej niż 100 Mbps z możliwością zwiększenia do 1 Gbps.
    a. Łącze musi posiadać ochronę przed atakami DDoS.
    b. Łącze nie może mieć miesięcznego limitu transferu danych.

9. Skonfigurowanie połączeń sieciowych pomiędzy poszczególnymi serwerami (maszynami wirtualnymi) zgodnie z wytycznymi dostarczonymi przez Zamawiającego.

10. Zestawienie połączenia typu site-to-site VPN z infrastruktury hostującej zapewnionej przez Wykonawcę do CPD Zamawiającego. Na potrzeby połączeń wewnętrznych i mechanizmów integracji Środowisk Platformy z komponentami w sieci Zamawiającego – co najmniej 2 tunele VPN.
11. Skonfigurowanie ochrony na styku z siecią Internet w warstwie sieciowej i aplikacyjnej zgodnie z wytycznymi dostarczonymi przez Zamawiającego.
12. Zapewnienie niezbędnych licencji, sprzętu i oprogramowania związanych z realizacją Umowy.
13. Skonfigurowanie i uruchomienie systemu do wykonywania kopii bezpieczeństwa wszystkich serwerów i bazy danych, kompatybilnego z system Zamawiającego (Veeam Backup & Replication) lub zapewnienie systemu równoważnego, umożliwiającego odtworzenie poszczególnych elementów środowiska Platformy na infrastrukturze Zamawiającego.
14. Przekazywanie kopii zapasowych i danych replikacji, dających możliwość odtworzenia Platformy w środowisku Zamawiającego (Veeam Backup & Replication). W przypadku braku kompatybilności tworzonych przez Wykonawcę kopii zapasowych z rozwiązaniem Zamawiającego, Wykonawca zobowiązany jest przekazać Zamawiającemu odpowiednie licencje lub w inny sposób umożliwić mu odtworzenie kopii zapasowych w CPD Zamawiającego, przez cały okres świadczenia usługi hostingu.
15. Zapewnienie replikacji danych wszystkich Środowisk z infrastruktury hostującej zapewnionej przez Wykonawcę do CPD Zamawiającego.
16. Wykonywanie kopii zapasowych maszyn wirtualnych hostujących Platformę.
17. Zapewnienie na okres trwania Umowy certyfikatu SSL odpowiadającego domenie: www.e-uslugi.mazowieckie.pl, o długości klucza co najmniej 2048 bitów podpisane przez autoryzowane centrum certyfikacji. Algorytm podpisu SHA-256.
18. W przypadku wystąpienia ataku, musi nastąpić eliminacja ruchu anonimizowanego (np. TOR, Open-Proxy, Anon-Proxy, Anon-VPN).
19. Należy wdrożyć algorytmy rozkładania ruchu pomiędzy wiele logicznych lokalizacji korzystających z danych zgromadzonych lokalnie (loadbalancing).
20. W przypadku dużego obciążenia atakowanej witryny Platformy, należy zastosować mechanizmy ochronne, które zapewnią ciągły dostęp do funkcjonalności Platformy.
21. Samodzielnego podjęcia działań zmierzających do zniwelowania zagrożenia w przypadku ataku oraz podjęcia działań zmierzających do odparcia ewentualnego ataku, w celu zniwelowania zagrożenia w przypadku jego wystąpienia.
22. Zapewnienie mechanizmu służącego do rejestracji zdarzeń w sieci teleinformatycznej wraz z archiwizacją zebranych logów (co najmniej za okres 6 miesięcy wstecz).

III. Minimalne wymagania sprzętowo-programowe

1. W ramach realizacji Usługi Wykonawca musi udostępniać maszyny wirtualne oraz oprogramowanie systemowe i narzędziowe o parametrach nie gorszych niż - określone w Tabeli 2.
2. Dane maszyn wirtualnych zostaną przekazane Zamawiającemu w formie plików kopii zapasowej w formacie systemu Veeam Backup And Replication lub obrazów maszyn wirtualnych na taśmach magnetycznych lub przesłane w postaci elektronicznej w inny uzgodniony z Zamawiającym sposób.
3. Wykonawca musi zapewnić niezawodność i ciągłość pracy serwerów (wysoką dostępność). W przypadku awarii serwera fizycznego musi następować automatyczne przełączenie zasobów w celu utrzymania ciągłości pracy Środowiska produkcyjnego gwarantując wymagany poziom SLA.
4. Wykonawca musi zapewnić redundancję dla wszystkich komponentów urządzeń serwerowych, w tym serwerów bazy danych i aplikacji wraz z zapewnieniem utworzenia klastrów niezawodnościowych.

5. Infrastruktura techniczno-systemowa dla Środowiska produkcyjnego musi zapewniać osiągnięcie następujących parametrów:
   a. RTO (Recovery Time Objective) - w przypadku Błędu krytycznego przywrócenie działania Środowiska nastąpi w ciągu maksymalnie 1 godziny zegarowej.
   b. RPO (Recovery Point Objective) - w przypadku Błędu krytycznego odtworzenie Środowiska wraz z danymi nastąpi według stanu maksymalnie 0 minut przed awarią (dokładność do ostatniej potwierdzonej transakcji).

6. Infrastruktura techniczno-systemowa dla Środowiska testowego i szkoleniowego musi zapewniać osiągnięcie następujących parametrów:

   a. RTO - w przypadku Błędu krytycznego przywrócenie działania Środowisk nastąpi w ciągu maksymalnie 1 godziny zegarowej.

   b. RPO - w przypadku Błędu krytycznego odtworzenie Środowisk wraz z danymi nastąpi według stanu maksymalnie do 1 godziny zegarowej przed awarią.

   Zamawiający może zażądać przeprowadzenia testów potwierdzających osiągnięcie powyższych parametrów RTO/RPO dla dowolnego ze Środowisk co najmniej raz na 3 miesiące.

7. Wykonawca musi zapewnić przestrzeń dyskową (macierz), która zapewni bezprzerwową dostępność (np. połączenie wielościeżkowe do serwerów wraz z redundantnymi interfejsami), RAID 0, 1, 5, 10, o parametrach nie gorszych niż określone w Tabeli nr 2.

8. Nośniki danych powinny być zorganizowane w sposób zapewniający dostęp do danych nawet w przypadku awarii części fizycznych nośników.

9. System kopii zapasowych musi umożliwiać wykonywanie cyklicznych kopii całych Środowisk (w tym co najmniej systemów operacyjnych i baz danych) zarówno na przestrzeń dyskową jak i taśmy magnetyczne. Wszystkie kopie zapasowe Platformy i jej modułów muszą być szyfrowane. Wymagana jest regularna realizacja usługi kopii zapasowej każdego Środowiska przy założeniu co najmniej:

   a. jednej kopii przyrostowej raz dziennie,

   b. jednej kopii pełnej w Okresie rozliczeniowym,

   c. retencji danych kopii zapasowej 60 dni w trakcie całego czasu trwania Umowy.

10. Wykonawca będzie przekazywał raport z każdej wykonanej kopii zapasowej na wskazany przez Zamawiającego adres e-mail oraz na koniec Okresu rozliczeniowego przekazywał zestawienia wszystkich wykonanych kopii zapasowych, w tym nieudanych.

11. Realizacja backupów nie może powodować przerw w dostępność Platformy ani w żadnym z komponentów.

12. Wykonawca będzie przekazywał pełne kopie zapasowe wszystkich Środowisk za każdy Okres rozliczeniowy, przesyłając szyfrowaną kopię na taśmie LTO (dopuszczalne standardy 6/7/8), maksymalnie w ciągu 5 dni od zakończenia Okresu rozliczeniowego, zawierającą dane z tego Okresu rozliczeniowego, na adres Zamawiającego wskazany w Umowie.

13. Wykonawca będzie przekazywał szyfrowane kopie przyrostowe wszystkich Środowisk do CPD Zamawiającego w cyklu tygodniowym, w każdą sobotę w sposób uzgodniony z Zamawiającym np. na serwer FTP/SFTP Zamawiającego. W przypadku nieudanej próby przesłania kopii, Wykonawca wykona ponowną próbę oraz powiadomi Zamawiającego o wystąpieniu problemów z przekazywaniem kopii wysyłając wiadomość na wskazany przez Zamawiającego adres e-mail.

14. Wykonawca ma obowiązek cyklicznego (nie rzadziej niż raz na kwartał) sprawdzenia skuteczności procedur kopii zapasowych danych, poprzez ich odtworzenie w innym środowisku i przeprowadzenie testów zgodności. Testy muszą obejmować co najmniej sprawdzenie możliwości uruchomienia wszystkich składników systemu oraz weryfikację zgodności danych. Wyniki każdorazowego testu muszą zostać przesłane Zamawiającemu w formie protokołu.

15. Zamawiający wymaga od Wykonawcy dostępu do systemu monitorowania umożliwiającego monitorowanie wszystkich parametrów usługi hostingu infrastruktury mogących wpłynąć na działanie poszczególnych Środowisk Platformy, w szczególności parametrów wydajności, niezawodności i pojemności (chwilowych i w okresie co najmniej: dnia, tygodnia, miesiąca / Okresu rozliczeniowego) w tym co najmniej danych takich jak: obciążenie procesora, użycie pamięci, użycia przepustowości interfejsów sieciowych, ilości odczytów i zapisów do podsystemu pamięci dyskowej dla każdego z udostępnych komponentów w ramach wszystkich Środowisk, wraz z możliwością konfiguracji poziomów ostrzegania, w tym zajętość dysków, dostępności usług, przepustowości łączy transmisyjnych. System musi posiadać możliwość konfiguracji powiadamiań e-mail.
16. Mechanizm monitorowania musi zapewnić wizualizację kluczowych parametrów w postaci tzw. dashboardu.
17. Środowisko wirtualne musi być zabezpieczone:
    a. Przez oprogramowanie uniemożliwiające instalację przez osoby nieuprawnione innego oprogramowania, w szczególności spowalniającego, utrudniającego lub uniemożliwiającego dostęp do Platformy.
    b. Jeśli wykonawca wskaże w ofercie, że zapewni konkretne rozwiązanie w zakresie zapewnienia modułu bezpieczeństwa filtrującego do poziomu aplikacji oraz usuwającego z pakietów http i https kody oraz exploity mogące zagrozić funkcjonowaniu Platformy i spójności zawartych w nim danych (WAF - ang. Web Application Firewall), zobowiązany jest wdrożyć je w ramach realizacji Umowy.

       W przypadku wskazania przez Wykonawcę rozwiązania opartego o FortiWeb, Zamawiający informuje, że może udostępnić już skonfigurowaną maszynę wirtualną. Jeżeli Wykonawca zdecyduje się skorzystać z udostępnienia skonfigurowanej maszyny wirtualnej, zobowiązany będzie do zapewnienia licencji FortiWeb, od momentu rozpoczęcia realizacji usługi.

    c. Jeśli wykonawca wskaże w ofercie, że zapewni konkretne rozwiązanie w zakresie zapewnienia dedykowanych (wydzielonych logicznie) maszyn z systemami firewall (w tym także warstwy aplikacji), IDS/IPS, monitoringu ruch sieciowego – next generation firewall, zobowiązany jest wdrożyć je w ramach realizacji Umowy.

       W przypadku wskazania przez Wykonawcę rozwiązania opartego o FortiGate, Zamawiający informuje, że może udostępnić już skonfigurowaną maszynę wirtualną. Jeżeli Wykonawca zdecyduje się skorzystać z udostępnienia skonfigurowanej maszyny wirtualnej, zobowiązany będzie do zapewnienia licencji FortiGate, od momentu rozpoczęcia realizacji usługi.
18. Jeśli wykonawca wskaże w ofercie, że zapewni dostęp do systemu służącego, do rejestracji zdarzeń w sieci (co najmniej na styku z siecią Internet) pozwalający na archiwizację zebranych logów za okres co najmniej ostatnich 6 miesięcy oraz agregacji danych statystycznych (logów dozwolonego ruchu sieciowego) co najmniej z modułu WAF i dedykowanych firewall logicznych, zobowiązany jest wdrożyć je w ramach realizacji Umowy.

    W przypadku wskazania przez Wykonawcę rozwiązania opartego o FortiAnalyzer, Zamawiający informuje, że może udostępnić już skonfigurowaną maszynę wirtualną. Jeżeli Wykonawca zdecyduje się skorzystać z udostępnienia skonfigurowanej maszyny wirtualnej, zobowiązany będzie do zapewnienia licencji FortiAnalyzer, od momentu rozpoczęcia realizacji usługi.

Tabela 1. Podsumowanie ilości komponentów

lp	Komponent	Ilość
1	Razem serwery wirtualne	24 szt.
2	Razem pamięć operacyjna	316 GB
3	Razem wirtualne procesory (dla procesora fizycznego o wydajności minimum 500 pkt w teście SPECint rate)	108 vCPU
4	Minimalna ilość adresów zewnętrznych IPv4	4 szt.
5	Minimalna ilość sieci wewnętrznych vLAN	10 szt.

Zastosowany system musi pozwalać na zwiększenie parametrów w zakresie ilości pamięci operacyjnej, ilości wirtualnych procesorów oraz przestrzeni dyskowej dla dowolnego Środowiska.

Tabela 2. Parametry techniczne środowisk wirtualnych

VM Name	vCPU	HDD [GB]	SSD [GB]	RAM GB	OS
Środowisko produkcyjne					
prod-1	4	250		8	CentOS 7 x64
prod-2	10	1000		48	CentOS 7 x64
prod-3	8	400	50	36	CentOS 7 x64
prod-4	8	400	50	36	CentOS 7 x64
prod-5	2	100		4	CentOS 7 x64
prod-6	8	260		28	CentOS 7 x64
prod-7	4	100		16	CentOS 7 x64
prod-8	4	100		16	CentOS 7 x64
prod-9	4	100	50	8	CentOS 7 x64
prod-10	2	40		2	CentOS 7 x64
Środowisko testowe					
test-1	2	40		4	CentOS 7 x64
test-2	6	60		16	CentOS 7 x64
test-3	4	100		16	CentOS 7 x64
test-4	4	32		2	CentOS 7 x64
test-5	4	40		6	CentOS 7 x64
test-6	4	60		10	CentOS 7 x64
test-7	4	60		8	CentOS 7 x64
Środowisko szkoleniowe					
szkol-1	2	40		4	CentOS 7 x64
szkol-2	4	60		10	CentOS 7 x64
szkol-3	4	100		16	CentOS 7 x64
szkol-4	4	32		2	CentOS 7 x64
szkol-5	4	40		6	CentOS 7 x64
szkol-6	4	60		6	CentOS 7 x64
szkol-7	4	60		8	CentOS 7 x64

IV. Wymagania dla ośrodka centrum przetwarzania danych Wykonawcy

1. Ośrodek przetwarzania musi posiadać zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo danych przetwarzanych. Ośrodek ponosi odpowiedzialność w zakresie bezpieczeństwa informacji przechowywanych na wykorzystanej infrastrukturze serwerowej.
2. Z uwagi na potrzebę wysokiej dostępności oferowanych usług Zamawiający oczekuje, aby udostępniona infrastruktura spełniała najwyższe standardy bezpieczeństwa informatycznego. Wymagania dla centrum przetwarzania danych, w którym gromadzone będą dane będące przedmiotem postępowania są obligatoryjne.

Tabela 3. Centrum przetwarzania danych.

OBIEKT I LOKALIZACJA	
L.p.	**Parametr lub kryterium**
1	Centrum przetwarzania danych musi być zlokalizowane na obszarze EOG. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na obszarze EOG.
2	Żadna procedura techniczna ani organizacyjna, w tym procedury zabezpieczania danych na wypadek awarii/katastrofy i odtwarzania po awarii/katastrofie nie może zakładać, ani dopuszczać transferu danych Zamawiającego poza obszar EOG.
3	Ogrodzony teren centrum przetwarzania danych.
4	Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.
5	Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej
6	Minimum 200 m oddalenie od linii wysokiego napięcia i elektrowni.
7	Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami.
8	Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Zamawiającemu od źródeł pól zakłócających (transformatory SN i WN).
9	Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf ma posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1.
10	Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie: budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.
11	Centrum musi być wyposażone w wydajną instalację klimatyzacji precyzyjnej pracującej w układzie N+1, która utrzymuje prawidłowe warunki pracy dla systemów zasilania oraz infrastruktury teleinformatycznej (temperatura pracy 15-25oC i wilgotność 30-60%). Zasilanie klimatyzacji musi odbywać się przez 2 redundantne tory zasilające.
WĘZŁY TELEKOMUNIKACYJNE	
1	Podłączenie w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym z zaimplementowanym protokołem BGP.

2	Dojścia połączeń do ośrodka przetwarzania danych wykonane dwoma niezależnymi trasami kablowymi.
3	Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi co najmniej 99,7%
ZASILANIE	
1	Dostępność roczna systemu zasilania co najmniej 99,7%.
2	Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT.
3	System zasilania awaryjnego UPS osobno na każdą linię zasilającą.
4	System zasilaczy awaryjnych UPS musi podtrzymać zasilanie urządzeń serwerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną.
5	Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy.
BEZPIECZEŃSTWO	
1	Wyposażenie w system kontroli dostępu (SKD).
2	Wyposażenie w system sygnalizacji włamania i napadu.
3	Wyposażenie w system sygnalizacji wykrywania wody i zalania.
4	Ochrona przez licencjonowaną firmę.
5	System CCTV zapewnia ciągły 365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu, monitorowane wszystkie pomieszczenia technologiczne.
6	System CCTV powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres co najmniej 21 dni.
7	System SKD dzieli centrum przetwarzania danych wraz z terenem na minimum 3 strefy dostępu z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I.
8	Dostęp do strefy I (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów).
9	Dostęp do strefy II (część administracyjno-biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem.
10	Dostęp do strefy III (część technologiczna) możliwy wyłącznie przy użyciu łącznie dwóch elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego.
11	System gaszenia powinien być bezpieczny dla sprzętu komputerowego i przetwarzanych danych.

12	Pomieszczenia centrum przetwarzania danych muszą być objęte: • systemami wykrywania pożaru i wczesnej detekcji dymu; • automatycznym systemem gaszenia opartym o gaz obojętny.
13	Ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.
14	System zarządzania bezpieczeństwem musi umożliwiać przypisywanie zidentyfikowanych incydentów bezpieczeństwa do natychmiastowej obsługi administracyjnej wraz z uruchomieniem procedury informowania. Zamawiający oczekuje powiadomień w tym zakresie co najmniej na wskazany przez Zamawiającego adres e-mail.
15	W pomieszczeniach centrum przetwarzania danych powinny być zainstalowane czujniki temperatury i wilgotności monitorujące w czasie rzeczywistym środowisko pracy serwerów i alarmujące pracowników centrum przetwarzania danych o przekroczeniach dopuszczalnych parametrów.
16	Centrum przetwarzania danych ma posiadać centralny system nadzoru umożliwiający pracownikom centrum nadzór nad instalacjami kontroli czynników ryzyka: • zasilania elektrycznego, • klimatyzacji precyzyjnej, • wentylacji, • systemu sygnalizacji pożaru, • systemu wczesnej detekcji dymu, • systemu gaszenia gazem, • systemu kontroli dostępu, w tym sygnalizacji włamania i napadu, • czujników parametrów środowiskowych, • CCTV, • systemu detekcji zalania.
17	Wykonawca musi posiadać wdrożone procedury postępowania w przypadku wykrycia nieprawidłowości w działaniu każdego z monitorowanych systemów.
MONITOROWANIE I RAPORTOWANIE usługi	
1	Wykonawca zapewni i udostępni Zamawiającemu system monitorowania działający w trybie 365/24/7, umożliwiający monitorowanie wszystkich parametrów usługi hostingu infrastruktury mogących wpłynąć na działanie poszczególnych Środowisk, w szczególności parametrów wydajności, niezawodności i pojemności (chwilowych i w okresie co najmniej: dnia, tygodnia, miesiąca / Okresu rozliczeniowego) w tym co najmniej danych takich jak: obciążenie procesora, użycie pamięci, ilość sesji, użycie przepustowości interfejsów sieciowych, ilości odczytów i zapisów do podsystemu pamięci dyskowej dla każdego z udostępnych komponentów w ramach wszystkich środowisk, wraz z możliwością konfiguracji poziomów ostrzegania, w tym zajętość dysków, dostępność usług, przepustowości łączy transmisyjnych, wysycenie łączy transmisyjnych. System musi posiadać możliwość konfiguracji powiadomień e-mail.
2	Wykonawca zapewni i udostępni Zamawiającemu elektroniczny system przyjmowania i obsługi zgłoszeń działający w trybie 365/24/7, zobowiązuje się rejestrować zgłoszenia, wykorzystując rozwiązania umożliwiające raportowanie wraz z danymi pozwalającymi co najmniej na śledzenie Czasu usunięcia Incydentu. Elektroniczny system zgłoszeń musi generować automatycznie wiadomość e-mail do Zamawiającego notyfikującą każde zgłoszenie przesłane Wykonawcy, w tym zgłoszenia wprowadzone przez stronę WWW, przez e-mail, przez telefon.
3	Wykonawca będzie dostarczał raporty tygodniowe i Raporty okresowe dotyczące monitorowanych parametrów opisanych w punkcie 1 i 2. Szczegóły i procedury raportowania zapisane zostały w Umowie.

Tabela 4. Naprawy i konserwacja sprzętu.

lp	Zakres
1	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.
2	Obsługa i naprawy muszą być dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami Ośrodka.
3	Obsługa musi usuwać nośniki danych przed przekazaniem sprzętu do naprawy.
4	Obsługa musi stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi).
5	Obsługa musi wykonywać przeglądy techniczne zgodnie z wymaganiami producenta sprzętu i procedurami wewnętrznymi Ośrodka.
6	Obsługa musi chronić Zamawiającego przed instalacją złośliwego oprogramowania.
7	Obsługa musi prowadzić rejestr incydentów, awarii, usterek.
8	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.

V. Warunki ciągłości działania SLA

1. Wykonawca zobowiązuje się świadczyć na rzecz Zamawiającego usługę hostingową dla każdego ze Środowisk w sposób ciągły, w systemie 24/7/365.
2. Wykonawca zobowiązuje się zabezpieczyć dostępność każdego ze Środowisk w okresie trwania Umowy na poziomie 99,7% w, przy czym:
    a. jednorazowa niedostępność każdego Środowiska oddzielnie nie przekroczy 1 godziny,
    b. łączna niedostępność każdego Środowiska oddzielnie dla każdego Okresu rozliczeniowego, nie może przekroczyć 2 godzin w okresie trwania Umowy, niezależnie od przyczyny,
    c. łączna roczna niedostępność każdego Środowiska oddzielnie, nie może przekroczyć 26 godzin i 17 minut w okresie trwania Umowy, niezależnie od przyczyny.
3. Na wykonanie przerwy technicznej (okna serwisowego) dla każdego z Środowisk oddzielnie, konieczne jest uzyskanie zgody Zamawiającego. Przerwa nie może przekroczyć 2 godzin i powinna następować w miarę możliwości w godzinach nocnych. W przypadku braku zgody na termin zaproponowany przez Wykonawcę, Zamawiający ma obowiązek zaproponować inny termin w ciągu 3 dni roboczych.
4. Wykonawca zobowiązuje się do przyjmowania zgłoszeń Incydentów w systemie obsługi zgłoszeń serwisowych Wykonawcy, całodobowo (24/7/365).
5. W przypadku Błędu krytycznego, Czas usunięcia Incydentu, czyli przywrócenie działania Środowisk nastąpi w przeciągu 1 godziny zegarowej od momentu zgłoszenia.
6. W przypadku Błędu niekrytycznego Środowiska Produkcyjnego, Czas usunięcia Incydentu, czyli przywrócenie działania nastąpi w przeciągu 8 godzin zegarowych od momentu zgłoszenia.
7. W przypadku Błędu niekrytycznego Środowiska Testowego i/lub Szkoleniowego, Czas usunięcia Incydentu, czyli przywrócenie działania nastąpi w ciągu maksymalnie 24 godzin zegarowych od momentu zgłoszenia.
8. Wykonawca zobowiązany jest do nadzoru nad działaniem usług hostingu, monitoringu oraz diagnozowania przyczyn niewłaściwego działania Środowisk leżących w obszarze usługi hostingu w sposób całkowicie samodzielny i bez angażowania Zamawiającego zapewniając SLA dla świadczone usługi na poziomie określonym w pkt V. 2.

9. Cykliczne informowanie Zamawiającego o wszelkich działaniach i wykrytych nieprawidłowościach udokumentowanych w raportach z realizacji usługi.

VI. Wymagania:

1. Wymagane certyfikaty dla Centrum Przetwarzania Danych:
    a. Aktualny certyfikat ISO 27001,

oraz

    b. TIER III Certification of Constructed Facility (The Uptime Institute),
    c. TIER III Design Documents (The Uptime Institute),

lub

    d. ANSI/TIA – 942 SITE na poziomie co najmniej Rated 3 (równoważny dla certyfikatów z pkt a i b).

2. Wymagania zespołu utrzymaniowego:
    a. Architekt IT - 1 osoba, która posiada doświadczenie zawodowe w opracowywaniu założeń i architektury systemów informatycznych.
    b. Administrator sieci - 1 osoba, która posiada doświadczenie zawodowe w administrowaniu urządzeniami sieciowymi.
    c. Administrator systemów wirtualnych - 2 osoby, które posiadają doświadczenie zawodowe w administrowaniu serwerami w środowisku wirtualnym.
    d. Administrator systemów operacyjnych lub administratora zabezpieczenia sieci - 1 osoba, która posiada doświadczenie zawodowe w administrowaniu systemami.

VII. Spis tabel