Specyfikacja zamówienia
W ramach zamówienia oczekuje się wykonania usługi o charakterze badawczo-rozwojowym, polegającej na wypożyczeniu elementów służących do budowy wirtualnej aparatury badawczej składającej się z następujących elementów:

Nazwa	Parametry	Ilość	Okres
vCPU	Intel Xeon@2.4 GHz	576	30 dni
RAM	GB	2304	
LAN	Połączenia miedzy serwerami i macierzą o przepustowości 10Gb/s	1	
HDD	GB /do 30000 IOPS/	10000	
IPv4	Adres zewnętrzny	2	
Internet	Łącze symetryczne 100 Mbps bez limitu transferu .	1	
Wirtualizacja	VMware		
Backup	Kopia całego środowiska realizowana raz na 24h, przechowywana 7 dni	1	
Zarządzanie	Konsola zarządzania całym środowiskiem	1	

Warunkiem koniecznym do złożenia oferty jest posiadanie aktualnego certyfikatu ISO 27001.
Dodatkowo oferent powinien spełniać następujące wymagania:

OBIEKT I LOKALIZACJA			
L.p.	Parametr lub kryterium	Wyeliminowanie zagrożenia	Wykonawca spełnia (TAK / NIE)
1	Ośrodek zlokalizowany na terenie Polski lub UE. Wszystkie dane będą gromadzone i przechowywane na terenie Polski lub UE.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR	
2	Ogrodzony teren obiektu	Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka	
3	Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub	Zagrożenienieprzerwanejpracyurządzeńserwerowychorazinnychurządzeńarchitektury ośrodka(elementyzasilania, agregaty)wwynikudziałańdziałaniasiłnatur	

	zalanie	y	
4	Minimum 500 m od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, łatwopalne również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych	Zagrożeniepowstaniasytuacjizagrażającyc h zdrowiulubżyciuosóbfizycznieobsługującyc h urządzenia,długotrwałegoskażeniaterenul ub długotrwałychdziałańsłużbzapobiegającyc h zdarzeniomkrytycznym(np.odcięcieterenu przezstrażpożarną,wojsko)	
5	Minimum1kmodmiejsc narażonychna wandalizmlub zamieszki(stadionyiobiekty sportowe,miejscorganizacjiimpr ez masowychnaminimum10tys. osób).	Zagrożeniedługotrwałegozablokowaniadró g dojazdowychdoośrodka,ryzyko niekontrolowanegozachowaniatłumów,ryz yko zamieszek,zniszczeń.	
6	Minimum200moddalenieodlinii wysokiegonapięciaielektrowni	Zagrożeniespowodowaniauszkodzeńw ynikającychzawariiliniiwysokiegonapię cia, ryzykowybuchów,ryzykopożarów.Zagr ożenie długotrwałegoograniczeniadostępudo ośrodkawynikającegoz wykonywanych napraw.	
7	Minimum15moddaleniaurządze ńkomputerowychudostępnionyc h Klientowi(Zamawiającemu)od źródełpól zakłócających (transformatorySNiWN).	Zagrożenieuszkodzeniaurządzeńidanych w wynikuniekorzystnegooddziaływaniapół zakłócającychpracęurządzeńelektrycznyc hi magnetycznych.	
8	Wysokośćtechnologiczna wewnątrz pomieszczenia serwerowni:min 3,5m- wysokośćmierzonaodpodłogitec hnicznejdo sufitu	Zagrożeniezachowaniaodpowiedniejcyrkul acjipowietrza,zachowaniastrefgorącejizim nej,zmianparametrówśrodowiskowych.	
9	Ośrodek spełniawymaganiaobowiązujący ch przepisóworazeuropejskichi polskichnormw zakresie:budownictwa, energetykiorazinstalacji elektrycznych, BHP, ochronyprzeciwpożarowej.	Przeciwdziałaniezagrożeniombudowlany m, pożarowymlubzagrożeniużyciaizdrowia ludziwwynikuniezastosowaniaprzepisów BHP,stosowaniaodrębnychod powszechnie stosowanychoznaczeń,błędówinstalacji energetycznej.	
WĘZŁY TELEKOMUNIKACYJNE			
1	Ośrodekpodłączonywpełni niezależnymidrogami światłowodowymidoconajmnie	Zagrożenieawariilub innejprzyczyny zaprzestaniaświadczeniausługtransmisj i danychprzezoperatora.	

	j dwóchróżnychoperatorów telekomunikacyjnychozasięgu krajowym		
2	Dojściapołączeńdo ośrodkawykonanedwomaniezależnymi trasamikablowymi.	Zagrożenieutratyciągłościkomunikacjidanych zośrodkiem.	
3	WęzełdostępowydosieciInternet dopiętydominimum2różnych operatorówz zaimplementowanym protokołemBGP	Zapewnienieniezawodnościijakościtransmisji danychwramachsieciInternet. Przeciwdziałaniezagrożeniuutratykomunikacji zsieciąInternet.	
4	WęzełdostępowydosieciInternet zezdublowanymiurządzeniamio gwarancjidostępnościrocznejusługi 99,98%	Zagrożenieutratyciągłościkomunikacji sprzętuzsieciąInternet.	
5	Węzełtelekomunikacyjny wyposażonywredundantnysystem firewall	Zagrożenieutratyzabezpieczeniasystemów informatycznychwwynikuuszkodzeniazapory ogniowej.	
6	Węzełtelekomunikacyjny wyposażonywredundantnysystem detekcjiiprewencjiwłamańzsieci.	Zagrożeniebezpieczeństwadanychwwyniku atakuinformatycznegonasystemy.	
	ZASILANIE		
1	Dostępnośćrocznasystemu zasilania99,99%	Zagrożenieciągłościpracyurządzeńi dostępnościurządzeń.	
2	Minimumdwiezewnętrznelinie zasilania	Zagrożeniezachowaniaciągłościzasilania w wynikuuszkodzenialiniizasilającejlub długotrwałegoprzywracaniaciągłości zasilania.	
3	System zasilaniaawaryjnegoUPS osobnonakażdąliniezasilającą	Zagrożeniedla zachowanianieprzerwanego zasilaniaurządzeńlubskróceniapracy urządzeńna zasilaniuawaryjnymponiżej czasubezpiecznego.	
4	Redundantny system agregatprądotwórczych	Zagrożeniebrakuzachowaniazasilania	
5	System zasilaczyawaryjnychUPS winienpodtrzymaćzasilanie urządzeńkomputerowych przeznaczonychdlaKlienta (Zamawiającego)przezprzynajmniej15minutodzanikunapięciainie krócejniżdoczasuuruchomieniasięagregatuijegosynchronizacjiz	Zagrożenieciągłościpracyurządzeńwwyniku niedostosowaniaczasupracyna zasilaniu awaryjnymdoczasureakcjinaawarięzasilaniaiuruchomieniaagregatów. Zagrożeniedlautratylubuszkodzeniadanych wwynikuniedostosowaniaczasupracy urządzeńdoczasubezpiecznegozamknięcia wykonywanychna	

	sieciąenergetyczną	urządzeniachprocesów.	
6	Agregatprądotwórczymaposiadaćzapaspaliwapozwalającyna autonomicznąpracębez koniecznościuzupełniania zbiornikówprzezconajmniej8 godzin.Agregatmusiumożliwiać uzupełnieniepaliwawtrakciejego pracy.	Zagrożeniepowstaniaprzerww zasilaniu wynikającychz zatrzymaniapracyagregatów.	
	BEZPIECZEŃSTWO		
1	Ośrodekwyposażonyw: systemtelewizji przemysłowej(CCTV),okresarchiwizacjimin.7dni, systemkontrolidostępu (SKD).	Zagrożeniebrakukontroliimonitorowania fizycznegodostępudo urządzeń.Zagrożenie brakumateriałówdowodowychwprzypadku naruszeniafizycznegobezpieczeństwa urządzeń.	
2	Ośrodek wyposażony w: Systemsygnalizacjiwłamaniai napadu, Systemwykrywaniawodyi zalania.	Zagrożeniebrakukontrolii reakcjina naruszeniebezpieczeństwafizycznegolub zalanieobiektu.	
3	SystemCCTV zapewniaciągły365/7/24dozórobszarówi rejestracjęzdarzeńz zachowaniem następującychparametrów funkcjonalnych: monitorowanewszystkiewejścia doobiektu–kamery wewnętrzne, monitorowanewszystkie pomieszczenia technologiczne.	Elementzapewnieniawczesnegowykrywaniai ostrzeganiaprzed zagrożeniemnaruszenia bezpieczeństwafizycznegoobiektuoraz zabezpieczeniamateriałudowodowegona wypadekzaistnienianaruszenia,wtym identyfikacjiosób.	
4	SystemCCTVpowinienzapewnić: rejestracjęzzapisemaktualnejdatyi godziny, archiwizacjazapisanegomateriału przezokresconajmniej7dni.	Elementzapewniającymożliwośćokreślenia chronologiizdarzeńzapisanychwsystemie monitorującymorazodtworzeniezapisu zdarzeńpo wykryciuzagrożeń.	
5	Systemgaszeniapowinienbyć bezpiecznydla ludziisprzętu komputerowego.	Zagrożeniepowstaniauszczerbkuna zdrowiu lubżyciuosóbwwynikufunkcjonowania systemugaszenia.	
6	Ściany, stropy Data center o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń data center o odporności ogniowej 60 minutowej.	Zapewnienieopornościogniowejdoczasu reakcjisłużbratowniczychwceluograniczenia skutkówwystąpieniapożaru.Przeciwdziałanie zagrożeniarozprzestrzenianiasiępożaru.	

MONITOROWANIE			
1	Systemprzyjmowaniazgłoszeńdotyczącychawariidziałający wtrybie365/24/7	Eliminacjazagrożeniabrakudziałańreakcjina zdarzeniakrytycznieprzypadającepozagodzinamipracybiurowej.	
2	Stałeicałodobowe(24/7/365) monitorowaniepoprawnościpracy infrastrukturyośrodkaiurządzeńkomputerowychudostępnianej Klientowi(Zamawiającemu). Pomiarymajądotyczyćminimum: wykresyprzebiegów temperatury, wykresprzebieguwilgotności.	Zagrożeniebrakukontroliparametrówpracy ośrodkaorazdługichreakcjiniekorzystne zmianywarunkówpracyurządzeń.	
3	Gromadzenielogówzdarzeńpracy urządzeńkomputerowych udostępnionychKlientowi (Zamawiającemu)	Zagrożeniebrakukontrolinadużytkowanymi urządzeniamikomputerowymiihistorii dowodowejpracyurządzeń.	