Pakiet C – załącznik 2

1. Serwer wraz z oprogramowaniem i akcesoriami – 2 szt.

Komponent	Minimalne wymagania
	Serwery wykorzystane zostaną do budowy wewnętrznego systemu informatycznego Zamawiającego.
Obudowa	Obudowa typu Rack o wysokości maksymalnej 1U, z możliwością instalacji min. 8 dysków 2.5” Hot-Plug w ramach jednej obudowy wraz z: - kompletem szyn umożliwiających montaż w standardowej szafie typu rack 19” z funkcjonalnością wysuwania serwera do celów serwisowych; - maskownicą panelu przedniego
Płyta główna	Płyta główna z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 4 sloty na pamięć RAM, z możliwością zainstalowania do 128 GB pamięci RAM.
Procesor	Oferowany serwer musi mieć zainstalowany minimum jeden procesor minimum 8-rdzeniowy wykonane w technologii x86-64, o wydajności pozwalającej na uzyskanie wyniku SPECspeed®2017_int_base nie mniejszego niż 14,1 pkt (dla oferowanego serwera, w pełni obsadzonego procesorami). Wyniki testu dla oferowanego serwera muszą być dostępne na stronie http://www.spec.org. (Załączyć wydruk ze strony do oferty – wydruk powinien zawierać pełen adres strony www)
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Pamięć RAM	Minimum 64GB pamięci RAM typu DDR4 o częstotliwości pracy 3200MHz. Pojedyncza kość pamięci RAM nie większa niż 16 GB. Na płycie głównej muszą znajdować się minimum 4 sloty przeznaczone na pamięć RAM. Zabezpieczenia pamięci: ECC.
Sloty PCI Express	Minimum jeden funkcjonalny slot PCIe generacji 4 o prędkości x16 oraz minimum jeden funkcjonalny sloty PCIe generacji 4 o prędkości x8.
Wbudowane porty	Minimum 3 porty USB (w tym co najmniej jeden w wersji 3.0). Ilość portów USB nie może zostać osiągnięta poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
Interfejsy	Minimum dwa interfejsy sieciowe 1Gb Ethernet. Minimum cztery interfejsy sieciowe 10Gb Ethernet na dodatkowych kartach sieciowych zamontowanych wewnątrz obudowy serwera. Na potrzeby funkcjonowania obydwu serwerów dostarczanych w ramach zamówienia wraz z zapewnieniem funkcjonowania zewnętrznego magazynu danych należy zapewnić połączenie na portach 10Gb Ethernet. Połączenie musi być zrealizowane redundantnie, niezależnie od awarii pojedynczego urządzenia. Wszystkie elementy funkcjonowania połączeń sieciowych muszą posiadać co najmniej dwa redundantne zasilacze. Połączenie musi być zapewnione w oparciu o rozwiązanie posiadające co najmniej 12MB pamięci na bufor pakietów, musi być w stanie obsłużyć co najmniej 250 tyś. adresów MAC, musi być w stanie obsłużyć co najmniej 255 sesji iSCSI i co najmniej 16 hostów iSCSI, co najmniej 4 tyś VLANów L2, co najmniej 500 VLANów L3, co najmniej 200 tyś IPv4 route.
Wewnętrzna pamięć masowa	Możliwość instalacji dysków twardych typu: SATA, SAS, SSD oraz dostępnych w ofercie producenta serwera.

	Zainstalowane minimum dwa dyski typu SSD SATA o pojemności nie mniejszej niż 480GB każdy, oznaczony profilem wykorzystania jako „mix use", z możliwością wymiany dysków podczas pracy serwera (hot plug).
Zewnętrzna pamięć masowa	Zespół serwerów wraz z oprogramowaniem musi być podłączony do zewnętrznego magazynu danych (zwany dalej ZMD), który należy dostarczyć w ramach zamówienia. ZMD musi być wyposażony w co najmniej 4 interfejsy 10Gb Ethernet, musi posiadać co najmniej 12 zatok na dyski twarde 3,5" z możliwością montażu dysków 2,5". Wysokość ZMD nie może być większa niż 2U. Zasilanie ZMD musi być realizowane za pomocą co najmniej 2 zasilaczy redundantnych o mocy co najmniej 560W pozwalających na ich wymianę w trakcie pracy ZMD. ZMD musi być wyposażony w co najmniej 8 dysków SSD SAS o pojemności co najmniej 960GB każdy o charakterystyce typu „read intensive" i prędkości co najmniej 12Gbps. ZMD musi być wyposażony w co najmniej 16GB pamięci RAM. ZMD musi obsługiwać dyski co najmniej typu NLSAS, SAS, SSD. ZMD musi być zgodny z listą sprzętu Vmware co najmniej dla wersji 8.0. Zarządzanie ZMD musi być możliwe za pomocą GUI HTML5 oraz CLI. Urządzenie według karty producenta nie może generować więcej niż 2000BTU.
Zasilacze	Redundantne zasilacze z funkcją hot plug o mocy zapewniającej poprawną pracę wszystkich zainstalowanych komponentów każdy wraz z kablami zasilającymi o mocy nie mniej niż 600W.
Zarządzanie serwerem	Niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port RJ-45 Gigabit Ethernet, umożliwiająca: - zdalny dostęp do graficznego interfejsu karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera; - bezpieczne, szyfrowane połączenie SSL; - możliwość podmontowania zdalnych wirtualnych napędów; - możliwość połączenia zdalnie do portu szeregowego; - bezpośrednie połączenie VNC do systemu operacyjnego; - wsparcie dla IPv6; - pełna informacja o stanie serwera: pomiar zużycia energii elektrycznej w czasie rzeczywistym, wykresy i dane historyczne, monitoring temperatury wraz z prezentacją graficzną na wykresie, monitoring wentylatorów, zasilania, pamięci, procesora, kart sieciowych i dysków twardych; - możliwość backupu konfiguracji serwera; - możliwość zrzutu z informacji w trakcie bootowania serwera oraz zrzutu ekranu w przypadku awarii serwera z poziomu systemu zarządzania serwerem; - możliwość ograniczenia mocy pobieranej przez serwer; - wsparcie dla SNMP v1, v2, v3; IPMI2.0, SSH; - integracja z Active Directory oraz LDAP; - możliwość zdalnego przesyłania plików; - wysyłanie alertów za pomocą email; Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI Express. Jeśli wymagana jest licencja do korzystania z funkcjonalności – należy ją dostarczyć.
Certyfikaty	- Serwer musi posiadać deklaracja CE (dokument załączyć do oferty).

	- Serwer winien znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów: Microsoft Windows Server 2019 x64 oraz Microsoft Windows Server 2022 x64. (Załączyć wydruk ze strony do oferty – wydruk powinien zawierać pełen adres strony www) - Serwer powinien być zgodny z wirtualizatorem VMware ESXi 8.0. (Załączyć wydruk ze strony do oferty – wydruk powinien zawierać pełen adres strony www)
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Gwarancja	1. Minimum 24 miesięcy gwarancji, realizowana w ciągu jednego dnia roboczego, możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub autoryzowanego partnera serwisowego. 2. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. 3. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach. 4. Urządzenie musi być wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy. 5. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta po podaniu numeru serwisowego urządzenia. 6. Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający będzie wymagał dostarczenia wraz z urządzeniem oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.
Zabezpieczenie danych	Wykonawca w ramach dostawy sprzętu jest zobowiązany do zabezpieczenia danych Zamawiającego na zewnętrznym systemie kopii zapasowych, który będzie integralną częścią środowiska jakie powstanie po uruchomieniu serwerów będących przedmiotem specyfikacji. Wykonawca musi zapewnić zabezpieczenie danych dla co najmniej 11 hostów (maszyny wirtualne Vmware), przestrzeń na dane w ilości 4TB, gwarancja czasu przechowywania min. 36 miesięcy. Zabezpieczenie danych musi cechować się następującymi parametrami minimalnymi: a. rozwiązanie musi umożliwiać odtworzenie całej maszyny wirtualnej jak również pojedynczych plików bezpośrednio z kopii zapasowej (bez konieczności przywracania w całości maszyny wirtualnej, aby odzyskać pojedynczy plik), niezależnie od systemu operacyjnego maszyny wirtualnej; b. rozwiązanie musi być wyposażone w wewnętrzne mechanizmy kompresji i deduplikacji - wykluczone jest stosowanie narzędzi innych, niż producenta rozwiązania systemu kopii zapasowej; c. mechanizm kompresji i deduplikacji musi być dostępny tylko dla danych nie zaszyfrowanych zarówno po stronie systemu operacyjnego maszyn wirtualnych i serwerów fizycznych oraz zaszyfrowanych przez dostarczony system kopii zapasowych; d. rozwiązanie musi mieć możliwość pracy z dowolnym typem urządzeń przechowujących dane w dowolnej ilości lokalizacji;

	e. rozwiązanie musi umożliwiać odkładanie kopii danych w różnych lokalizacjach geograficznych i logicznych, przy zachowaniu pełnej funkcjonalności systemu; f. rozwiązanie musi umożliwiać pełne uruchomienie maszyny wirtualnej z kopii zapasowej w przypadku awarii oraz równoczesną realizację jej przywracania. Równolegle muszą mieć możliwość działać dwa procesy: 1) proces przywracania maszyny wirtualnej z kopii zapasowej, 2) proces jej poprawnego, pełnego funkcjonowania w trakcie operacji przywracania; g. rozwiązanie musi umożliwiać przywracanie pojedynczych elementów aplikacyjnych z kopii zapasowych bez konieczności wcześniejszego przywrócenia całej maszyny wirtualnej. Do tych elementów zaliczają się co najmniej: pojedyncze wiadomości email lub pojedyncze wiersze i tabele baz danych. Miejsce przechowywania danych musi spełniać wymogi minimalne opisane w tabeli 1.1.
Oprogramowanie - system operacyjny	Windows Server 2022 Standard – licencja na wszystkie rdzenie lub równoważny: Licencje na serwerowy system operacyjny przypisane do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego. 1. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 2. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 3. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 4. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 5. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 6. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 7. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

	8. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 9. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 10. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 11. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 12. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 13. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 14. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 15. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 16. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 17. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 18. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 19. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 20. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 21. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

	ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wsparcie dla algorytmów Suite B (RFC 4869), l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Możliwa liczba maszyn wirtualnych w ramach licencji: 2. v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 23. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję

	poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 24. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 25. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 26. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 27. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Oprogramowanie - licencje użytkowe	1. Vmware vSphere 8 Essentials Kit – wersja na maksymalnie 3 hosty (maksymalnie 2 procesory na każdy host). Wsparcie na 36 miesięcy. 2. Jedna licencja Oracle Database Standard Edition One 1CPU. Licencją ma zostać objęty tylko jeden z dwóch serwerów rack. Typ licencji – wieczysta. Okres wsparcia min. 12 miesięcy.
Wdrożenie	1. Montaż dostarczonych urządzeń w szafach i ich połączenie. 2. Konfiguracja wszystkich komponentów sprzętowych i programowych, portów, interfejsów. 3. Instalacja oprogramowania w tym systemów VMware ESXi na dostarczonym sprzęcie. 4. Zabezpieczenie danych powstałego środowiska na bazie dostarczonego sprzętu. 5. Dostarczenie dokumentacji powykonawczej wykonanego środowiska z uwzględnieniem architektury fizycznej i logicznej całości rozwiązania.

Tabela 1.1. Miejsce przechowywania danych na potrzeby ich zabezpieczenia

L.p.	Parametr lub kryterium	Wyeliminowanie zagrożenia
OBIEKT I LOKALIZACJA		
1	CPD oraz jego zasoby zlokalizowane na terenie Rzeczypospolitej Polskiej.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium Rzeczypospolitej Polskiej. Brak spełnienie wymagań RODO / GDPR.
2	CPD posiada ogrodzony zamknięty teren wraz z ograniczoną strefą wejść.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji).
3	CPD jest usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji) w wyniku działań działania sił natury.

4	CPD jest położony nie mniej niż 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania. Wysoka intensywność oddziaływania sytuacji krytycznych.
5	CPD jest oddalony nie mniej niż 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych.	Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko). Zagrożenie fizycznego uszkodzenia infrastruktury IT oraz innych urządzeń w skutek eksplozji zewnętrznej.
6	CPD jest oddalony nie mniej niż 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych dla 10 tys. osób i więcej).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.
7	CPD nie posiada ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z urządzeniami serwerowymi.	Zagrożenie przecieków, zalania infrastruktury IT lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).
8	CPD posiada nie mniej niż 15 metrów oddalenia urządzeń serwerowych udostępnionych Zamawiającemu od źródeł pól zakłócających takich jak transformatory SN i WN.	Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pół zakłócających pracę urządzeń elektrycznych i magnetycznych.
9	CPD posiada pomieszczenia serwerowe o wysokości nie mniejszej niż 3 metra - wysokość mierzona od podłogi technicznej do sufitu pomieszczenia - w których będą znajdowały się urządzenia serwerowe udostępnione Zamawiającemu.	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych. Zagrożenie uszkodzenia lub utraty danych na wypadek uruchomienia systemu gaszenia.
10	CPD posiada podłogę techniczną w pomieszczeniu z serwerami o wysokości nie mniejszej niż 1 metr.	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.

11	CPD spełnienia wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie: budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej.
WĘZŁY TELEKOMUNIKACYJNE		
1	CPD posiada połączenie światłowodowe z niezależnymi operatorami telekomunikacyjnymi, w tym nie mniej niż 2 operatorów o zasięgu krajowym jest podłączonych niezależnymi drogami światłowodowymi.	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora zewnętrznego.
2	Dojścia połączeń CPD wykonane są dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.
3	CPD posiada węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP.	Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.
4	CPD posiada węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%.	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.
5	CPD posiada węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.
6	CPD posiada węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.
ZASILANIE ENERGETYCZNE		
1	CPD posiada dostępność roczną systemu zasilania energetycznego na poziomie nie niższym niż 99,99%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.

2	CPD posiada nie mniej niż dwie niezależne linie zasilania dostępne dla infrastruktury IT.	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.
3	CPD posiada system zasilania awaryjnego UPS osobno na każdą linię zasilającą.	Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego.
4	CPD posiada redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.
5	System zasilaczy awaryjnych UPS w CPD gwarantuje podtrzymanie zasilania urządzeń serwerowych oraz infrastruktury towarzyszącej, przeznaczonej dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatów i ich synchronizacji z siecią energetyczną.	Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów.
6	Agregaty prądotwórcze PDC posiadają zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy.	Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów.
BEZPIECZEŃSTWO		
1	CPD jest wyposażone w system sygnalizacji włamania i napadu, system wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.
2	CPD posiada ochronę całego obiektu realizowaną przez profesjonalną zewnętrzną licencjonowaną firmę ochrony mienia. Ochrona realizowana jest w trybie 24/7.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.
3	CPD posiada system CCTV, który zapewnia ciągły 24/7 dozór obszarów i rejestrację zdarzeń z zachowaniem	Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz

	następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne.	zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób.
4	System CCTV w CPD powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres nie krótszy niż 21 dni.	Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.
5	System CPD (System Kontroli Dostępu) w PDC obejmuje nie mniej niż cztery strefy dostępu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po terenie i obiekcie.
6	Dostęp do strefy I (teren w otoczeniu obiektu) w CPD podlega identyfikacji na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów) wkraczających na ogrodzony teren w otoczeniu obiektu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
7	Dostęp do strefy II (część biurowa obiektu) w CPD podlega identyfikacji na podstawie dokumentu tożsamości ze zdjęciem.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
8	Dostęp do strefy III (strefa technologiczna) w CPD możliwy jest wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
9	Dostęp do strefy IV (pomieszczenia ze sprzętem serwerowym Zamawiającego) w PDC możliwy jest wyłącznie przy użyciu łącznie 2 elementów identyfikacji: SKD, osobistej karty identyfikacyjnej, hasła (kodu) lub elementu biometrycznego.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.

10	CPD posiada system gaszenia bezpieczny dla ludzi i sprzętu komputerowego oraz serwerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.
11	CPD posiada ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru.
MONITORING		
1	CPD posiada elektroniczny system przyjmowania zgłoszeń dotyczących awarii dostępny w trybie 24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.
2	CPD posiada stałe i całodobowe 24/7 monitorowanie poprawności pracy infrastruktury i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności.	Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń.
Certyfikacja obiektu		
1	CDP posiada posiadamy aktualny certyfikat ISO 27001 na usługi cloud computing i backup	
2	CDP posiada posiadamy aktualny certyfikat ISO 27017 na usługi cloud computing i backup	
3	CDP posiada posiadamy aktualny certyfikat ISO 22301 na usługi cloud computing i backup	
4	CDP posiada aktualny certyfikat TIER III dokumentacji	Zapewnienie stabilności i ciągłości działania usługi.
5	CDP posiadamy aktualny certyfikat TIER III infrastruktury	Zapewnienie stabilności i ciągłości działania usługi.