**Załącznik nr 1F do swz/załącznik nr 2 do umowy dla części I zamówienia**

# Szczegółowy opis przedmiotu zamówienia Część I zamówienia

Dostawa infrastruktury teleinformatycznej do uruchomienia systemu EZD RP wraz z wdrożeniem w sześciu Jednostkach Organizacyjnych Województwa Małopolskiego wraz z zapewnieniem wsparcia. Wymagania dla systemu EZD RP (dla wersji produkcyjnej i testowej) dostępne są na stronie producenta rozwiązania (<https://podrecznik.ezdrp.gov.pl/>). Rozmieszczenie fizyczne i ilościowe sprzętu wraz z oprogramowaniem znajduje się w pkt VIII ppkt 1.

# Niniejsza część zamówienia obejmuje:

* 1. Dostawę i wdrożenie 6 serwerów (konfiguracja I) wraz z wirtualizatorem i licencją na system operacyjny,
  2. Dostawę i wdrożenie 6 serwerów (konfiguracja II) wraz z oprogramowaniem przeznaczonym do wykonania kopii zapasowej
  3. Dostawę i wdrożenie 6 zapór sieciowych wraz z licencjami i oprogramowaniem,
  4. Dostawę i wdrożenie 12 przełączników sieciowych wraz z licencjami i oprogramowaniem,
  5. Dostawę i wdrożenie 6 zestawów podtrzymywania energii,
  6. Dostawę i wdrożenie 6 szaf teletechnicznych (szaf RACKowych),
  7. Zapewnienie instalacji i wsparcia,
  8. Szkolenie.

# Opis minimalnych parametrów technicznych dla 6 serwerów (konfiguracja I) wraz z wirtualizatorem i licencją na systemy operacyjne

|  |  |  |
| --- | --- | --- |
| Minimalne parametry techniczne serwera | Obudowa i okablowanie | * Maksymalnie 2U z osprzętem niezbędnym do zainstalowania w szafie typu RACK (np. maskownica) * Obudowa musi posiadać komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie obudowy do celów serwisowych, * Obudowa musi posiadać wskaźniki sygnalizacji LED, które wskazują minimum:   + włączanie/status zasilania,   + identyfikacja serwera,   + aktywność łącza sieciowego, * Oferowana obudowana musi zapewniać ochronę przed nieautoryzowanym dostępem do dysków poprzez dedykowaną ramkę zabezpieczającą |
| Płyta główna i chipset | * Dedykowana płyta główna obsługująca i umożliwiająca instalację dwóch procesorów. * Płyta główna musi posiadać dedykowany przez producenta chipset do pracy w serwerach dwuprocesorowych. |
| Procesor | * Zainstalowane minimum dwa procesory x86, każdy z procesorów musi posiadać minimum 24 rdzeni/48 wątków, * Zainstalowane procesory muszą umożliwić osiągnięcie wyniku minimum 430 punktów w teście SPECrate2017\_int\_base (SPEC CPU®2017 Integer Rate Result), dostępnym na stronie [www.spec.org](http://www.spec.org) dla konfiguracji dwuprocesorowej. |
| Pamięć operacyjna RAM | * Zainstalowane minimum 256 GB DDR5 * Serwer musi zapewniać rozbudowę pamięć RAM do minimum 1 TB DDR5 |
| Kontroler RAID | * Zainstalowany sprzętowy kontroler dyskowy posiadający minimum 4GB pamięci cache. * Oferowany sprzętowy kontroler musi umożliwiać konfigurację RAID: 0, 1, 5, 6, 10, * Oferowany sprzętowy kontroler musi zapewniać wsparcie dla dysków SAS/SATA HDD, SAS/SATA SSD oraz NVMe |
| Przestrzeń dyskowa | * Możliwość instalacji dysków 2.5” SAS/SATA HDD, SAS/SATA SSD oraz NVMe w obudowie serwera. * Zainstalowane minimum dwa dyski NVMe o pojemności minimum 450 GB, służące do zainstalowania wirtualizatora, * Zapewnienie minimum pojemności netto 11TB przy zastosowani mechanizmu RAID6 z wykorzystaniem dysków SSD lub NVMe, przy wykorzystaniu dysków o pojemności minimum 3.7 TB, * Dyski NVMe o pojemności minimum 450 GB, służące do zainstalowania wirtualizatora nie będą wliczały się do powyższej puli RAID 6 (która musi zapewnić minimum 11 TB pojemności netto), * Zaoferowane rozwiązane umożliwi instalację dodatkowych dysków SSD lub NVMe w obudowie serwera i umożliwi rozszerzenie powyższej puli RAID 6 o minimum 10 dodatkowych dysków SSD lub NVMe. |
| Zarządzanie i obsługa techniczna | Serwer musi być wyposażony w działającą funkcję zdalnego zarządzania niezależną od zainstalowanego na serwerze systemu operacyjnego posiadającą dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:   * włączenie, wyłączenie i restart serwera, * zdalny dostęp do graficznego interfejsu Web karty zarządzającej, * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera), * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, * wsparcie dla SNMP, IPMI 2.0, * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, * możliwość podłączania wirtualnych napędów CD/DVD/ISO, * min. 2 porty USB w tym minimum 1 zewnętrzny port USB 3.0, * minimum 1 port video (analogowy lub cyfrowy), * Jeśli wymagana jest licencja - musi być dostarczona. |
| Bezpieczeństwo | * Obsługa minimum TPM 2.0, secure boot * Urządzenie musi oferować Secure Boot. |
| Interfejsy sieciowe | * Minimum czerty porty umożliwiające instalację wkładek minimum SFP/SFP+ umożliwiające uzyskanie minimum prędkości 10/25 Gbps Ethernet * Minimum 1 port Ethernetowy, umożliwiający zdalne zarządzanie serwerem |
| Zasilanie i chłodzenie | * Urządzenie musi posiadać redundantne wentylatory hot-swappable. * Oferowane urządzenie musi posiadać minimum dwa dedykowane zasilacze hot-swappable wraz z kablami zasilającymi, * Zaoferowane zasilacze muszą mieć sprawność o klasie minimum platinium |
| Oprogramowanie | * Zaoferowany serwer powinien być kompatybilny z zaoferowanym oprogramowaniem wirtualzacyjnym, * Wszystkie licencje powinny zostać umożliwiające np. zdalne zarządzenie serwerem powinno być dostarczone wraz z serwem |
| Gwarancja producenta | * minimum 60 miesięcy gwarancji wraz serwisem producenta, z czasem reakcji do następnego dnia roboczego (next business day) od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 * dyski bezzwrotne w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego |
| Certyfikaty | * Urządzenie musi spełniać wymagania i normy dyrektyw Unii Europejskiej i polskiego prawa dotyczącego zdrowia, bezpieczeństwa i ochrony środowiska. |
| Minimalne parametry i opis rozwiązania zapewniającego wirtualizację wraz z licencją na systemy operacyjne | * Licencja/Subskrypcja na oprogramowanie wirtualizacyjne, które będzie pełnić rolę hypervisora dla serwera dla maszyn wirtualnych. Zamawiający dopuszcza rozwiązanie, aby zaoferowany wirtualizator mógł pełnić rolę hypervisora dla maszyn wirtualnych oraz środowiska kubernetes dla kontenerów. * Licencja/Subskrypcja musi umożliwiać zarządzanie i uruchamianie maszyn wirtualnych (VM) oraz zainstalowanie nieograniczonej ilości systemów operacyjnych na okres minimum 60 miesięcy. W przypadku, gdy został zaoferowany wirtualizator, który może pełnić rolę hypervisora dla maszyn wirtualnych oraz środowiska kubernetes dla kontenerów musi również umożliwiać zarządzanie i uruchamianie maszyn wirtualnych (VM) oraz kontenerów zainstalowanie nieograniczonej ilości systemów operacyjnych na okres minimum 60 miesięcy. * Po ustaniu licencji musi być zapewniona możliwość korzystania z rozwiązania oraz systemów zainstalowanych na zaoferowanym rozwiązaniu. Zamawiający dopuszcza aby w ramach gwarancji na dostarczoną infrastrukturę Wykonawca, po ustaniu licencji na zaoferowany wirtualizator wdroży i przemigruje wszystkie maszyny wirtualne wraz kontenerami (jeśli występują) na wirtualizator, który będzie dostępny w ramach licencji do komercyjnego użytkowania. * Zaoferowane rozwiązanie musi umożliwić pracę na serwerze w opisanej konfiguracji z wykorzystaniem wszystkich jego zasobów sprzętowych, a także powinno być w pełni kompatybilne i wykorzystywać zasoby serwera. * Rozwiązanie musi posiadać graficzny interfejs GUI oraz interfejs command line (CLI) do zarządzania. * Mechanizmy wirtualizacji muszą umożliwiać tworzenie maszyn wirtualnych opierających się m.in. na:   + systemach operacyjnych z rodziny Microsoft Windows Server w wersji minimum 2016/2019/2022/2025   + systemach operacyjnych w wersji minimum Windows 10/11   + systemach operacyjnych z rodziny Linux w wersji minimum Red Hat Linux 8, Red Hat Linux 9, Ubuntu Server 18, Ubuntu Server 22, Ubuntu Server 24, SLES 15 * Wirtualizator musi mieć możliwość uruchomienia zdalnej sesji (konsoli) m.in. wirtualnej maszyny utworzonej na tym wirtualizatorze. * Wirtualizator musi zapewniać monitoring wykorzystania podstawowych zasobów:   + vCPU,   + Network,   + Storage. * Wirtualizator musi zapewniać tworzenie snapshot-ów (migawek) maszyn wirtualnych. * Witalizator musi umożliwiać uruchomienia środowiska bazującego na rozwiązanych kontenerowych w tym jednowęzłowego klastra Kubernetes, * Wirtualizator musi umożliwiać m.in. tworzenie, usuwanie i zarządzanie dysków wirtualnych wykorzystywanych przez maszyny wirtualne, * Wirtualizator musi umożliwiać podłączenie wirtualnego napędu w celu uruchomienia obrazu płyty m.in. w formacie ISO, * Wirtualizator musi umożliwić zarządzanie przestrzenią dyskową (m.in. zarządzanie przestrzenią gdzie składowane są pliki maszyn wirtualnych, zarządzanie LUNami, zarządzanie pamięcią SAN), * Wirtualizator musi zapewniać możliwość importowania i klonowania maszyn wirtualnych, * Wirtualizator musi zapewniać funkcję przenoszenie maszyn wirtualnych pomiędzy węzłami klastra bez konieczności wyłączania maszyny wirtualnej z zapewnieniem ciągłości działania, * Systemy operacyjne zainstalowane na wirtulizatorze muszą mieć możliwość uruchomienia usług m.in. NFS, RabbitMQ, Redis na niezależnych maszynach wirtualnych, * Wirtualizator musi umożliwić korzystanie z urządzeń podłączonych do portów USB serwera w maszynie wirtualnej, * Rozwiązanie musi mieć możliwość instalacji i pracy w środowiskach tzw. disconnected bez dostępu do sieci Internet * Rozwiązanie musi wspierać działanie w trybie wysokiej dostępności oraz umożliwiać uruchomienie aplikacji w trybie wysokiej dostępności * Rozwiązanie, musi mieć funkcjonalność tworzenia wirtualnych sieci, przełączników, itp. * Rozwiązanie musi zapewniać uwierzytelnianie dostępu do rozwiązani z wykorzystaniem minimum: OpenID Connect, LDAP, MS Active Directory, 3rd party IdP, * Rozwiązanie musi posiadać funkcjonalność zarządzenia cyklem życia maszyn wirtualnych, w tym ich tworzenie, uruchamianie, zatrzymywanie, klonowanie i usuwanie, * Rozwiązanie musi posiadać zcentralizowane zarządzanie maszynami wirtualnymi i kontenerami (w przypadku, gdy wirtualizator wspiera natywną konfigurację) w jednym interfejsie poprzez konsolę webową oraz narzędzia linii poleceń, * Rozwiązanie musi posiadać możliwość tworzenia replik maszyn wirtualnych i ich przechowywania w celu odzyskiwania po awarii (Disaster Recovery), * Rozwiązanie musi posiadać możliwość tworzenia, usuwania i zarządzania dyskami wirtualnymi wykorzystywanymi przez maszyny wirtualne.   Wraz z rozwiązaniem hypervisora/wirtualizatora musi zostać dostarczona licencja (np. po przez przypisanie licencji do zaoferowanego wirtualizatora) umożliwiająca zainstalowanie nieograniczonej ilości systemów operacyjnych Red Hat Enterprise Linux w formie maszyn wirtualnych na okres minimum 60 miesięcy.  Rozwiązanie to powinno zostać dostarczone ze wszystkimi licencjami oraz wsparciem producenta na okres minimum 60 miesięcy – nie jest akceptowane wsparcie typu „community support”, oferowane przez społeczność jego użytkowników lub wsparcie oferowane wyłącznie przez dostawcę. Po ustaniu licencji musi być zapewniona możliwość korzystania z systemów zainstalowanych na zaoferowanym rozwiązaniu.  Zaoferowane oprogramowanie musi umożliwiać:   * produkcyjnego wykorzystania rozwiązania w środowisku Zamawiającego * instalacji najnowszych wersji oprogramowania (w tym prawo do upgrade); * dostępu do aktualizacji i poprawek oprogramowania (patches, bug fixes, updates); * dostępu do bazy wiedzy oprogramowania przez dedykowany portal kliencki; * możliwości przenoszenia licencji na nowe serwery/urządzenia w ramach wymiany starych technologii na nowe w ramach tej samej organizacji; * dostępu i pełnej funkcjonalności portalu, w tym rejestracji subskrypcji z uprawnieniami administratora dla subskrypcji dostarczanych w ramach zamówienia gwarantowanego oraz realizowanych w ramach prawa opcji. | |

# Opis minimalnych parametrów technicznych dla 6 serwerów (konfiguracji II) wraz z oprogramowaniem przeznaczonym do wykonania kopii zapasowej:

|  |  |  |
| --- | --- | --- |
| Minimalne parametry techniczne serwera | Obudowa i okablowanie | * Maksymalnie 2U z osprzętem niezbędnym do zainstalowania w szafie typu RACK (w tym m.in. komplet wysuwanych szyn do montażu, organizator kabli, maskownica), * Obudowa musi posiadać komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie obudowy do celów serwisowych, * Obudowa musi posiadać wskaźniki sygnalizacji LED, które wskazują minimum:   + włączanie/status zasilania,   + identyfikacja serwera,   + aktywność łącza sieciowego, * Oferowana obudowana musi zapewniać ochronę przed nieautoryzowanym dostępem do dysków poprzez dedykowaną ramkę zabezpieczającą, * Komplet patch cordów światłowodowych o długości minimum 2 metry. |
| Płyta główna i chipset | * Dedykowana płyta główna obsługująca i umożliwiająca instalację dwóch procesorów. * Płyta główna musi posiadać dedykowany przez producenta chipset do pracy w serwerach dwuprocesorowych. |
| Procesor | * Zainstalowane minimum dwa procesory x86, każdy z procesorów musi posiadać minimum 12 rdzeni/24 wątki * Zainstalowane procesory muszą umożliwić osiągnięcie wyniku minimum 190 punktów w teście SPECrate2017\_int\_base (SPEC CPU®2017 Integer Rate Result), dostępnym na stronie [www.spec.org](http://www.spec.org) dla konfiguracji dwuprocesorowej. |
| Pamięć operacyjna RAM | * Zainstalowane minimum 64 GB DDR5 * Serwer musi zapewniać rozbudowę pamięć RAM do minimum 512 GB DDR5 |
| Kontroler RAID | * Zainstalowany sprzętowy kontroler dyskowy posiadający minimum 4GB pamięci cache. * Oferowany sprzętowy kontroler musi umożliwiać konfigurację RAID: 0, 1, 5, 6, 10 * Oferowany sprzętowy kontroler musi zapewniać wsparcie dla dysków SAS/SATA HDD, SAS/SATA SSD oraz NVMe |
| Przestrzeń dyskowa | * Możliwość instalacji dysków 2.5” SAS/SATA HDD, SAS/SATA SSD oraz NVMe w obudowie serwera. * Zainstalowane minimum dwa dyski NVMe o pojemności minimum 450 GB, służące do zainstalowania oprogramowania kopii zapasowej (i ewentualnym systemem operacyjnym) * Zapewnienie minimum pojemności netto 11TB przy zastosowani mechanizmu RAID6 z wykorzystaniem dysków SSD lub NVMe, przy wykorzystaniu dysków o pojemności minimum 3.7 TB, * Dyski NVMe o pojemności minimum 450 GB, służące do zainstalowania oprogramowania kopii zapasowej (i ewentualnym systemem operacyjnym) nie będą wliczały się do powyższej puli RAID 6 (która musi zapewnić minimum 11 TB pojemności netto), * Zaoferowane rozwiązane umożliwi instalację dodatkowych dysków SSD lub NVMe w obudowie serwera i umożliwi rozszerzenie powyższej puli RAID 6 o minimum 10 dodatkowych dysków SSD lub NVMe. |
| Zarządzanie i obsługa techniczna | Serwer musi być wyposażony w działającą funkcję zdalnego zarządzania niezależną od zainstalowanego na serwerze systemu operacyjnego posiadającą dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:   * włączenie, wyłączenie i restart serwera, * zdalny dostęp do graficznego interfejsu Web karty zarządzającej, * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera), * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, * wsparcie dla SNMP, IPMI 2.0, * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, * możliwość podłączania wirtualnych napędów CD/DVD/ISO, * min. 2 porty USB w tym minimum 1 zewnętrzny port USB 3.0, * minimum 1 port video (analogowy lub cyfrowy), * Jeśli wymagana jest licencja - musi być dostarczona. |
| Bezpieczeństwo | * Obsługa minimum TPM 2.0, secure boot * Urządzenie musi oferować Secure Boot. |
| Interfejsy sieciowe | * Minimum czerty porty umożliwiające instalację wkładek minimum SFP/SFP+ umożliwiające uzyskanie minimum prędkości 10/25 Gbps Ethernet * Minimum 1 port Ethernetowy, umożliwiający zdalne zarządzanie serwerem |
| Zasilanie i chłodzenie | * Urządzenie musi posiadać redundantne wentylatory hot-swappable. * Oferowane urządzenie musi posiadać minimum dwa dedykowane zasilacze hot-swappable wraz z kablami zasilającymi * Zaoferowane zasilacze muszą mieć sprawność o klasie minimum platinium |
| Oprogramowanie | * Zaoferowany serwer powinien być kompatybilny z zaoferowanym oprogramowaniem (i ewentualnym systemem operacyjnym, na którym oprogramowanie backupowe zostało zainstalowane) * Wszystkie licencje powinny zostać umożliwiające np. zdalne zarządzenie serwerem powinno być dostarczone wraz z serwem |
| Gwarancja i wsparcie | * minimum 60 miesięcy gwarancji wraz serwisem producenta, z czasem reakcji do następnego dnia roboczego (next business day) od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 * dyski bezzwrotne w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego |
| Certyfikaty | * Urządzenie musi spełniać wymagania i normy dyrektyw Unii Europejskiej i polskiego prawa dotyczącego zdrowia, bezpieczeństwa i ochrony środowiska. |
| Minimalne parametry techniczne serwera i opis rozwiązania softwarowego do backupu | Licencja na oprogramowanie backupowe wraz z licencją na systemem operacyjnym wymagany do uruchomienia rozwiązania backupowego (jeśli jest wymagane) umożliwiające utworzenie i przechowywanie kopii zapasowej maszyn wirtualnych oraz rozwiązań bazujących na kontenerach. Zaoferowane oprogramowanie powinno być kompatybilne z zaoferowanym serwerem.  Oprogramowanie wykonujące kopię bezpieczeństwo musi:   * wspierać usługi przechowywania danych takich jak:   + baza danych PostgreSQL,   + baza danych MySQL,   + baza danych Microsoft SQL Server   + serwer NFS * wspierać rozwiązania:   + Openshift w wersji min. 4.11,   + Proxmox od wersji minimum 5.2,   + VMWare, * Umożliwić wykonania kopii zapasowych na systemach z rodziny:   + Microsoft Windows 2016/2019/2022/2025   + Red Hat Enterprise Linux 8 oraz Red Hat Enterprise Linux 9   + Ubuntu Server 18, Ubuntu Server 22, Ubuntu Server 24 * Rozwiązanie backupowe musi wspierać wykonywanie kopii zapasowych wirtualnych maszyn z zainstalowaną instancją RKE2 lub natywnie kubernetesa. * Oferowane rozwiązanie musi wspierać backup na bibliotekę taśmową LTO. * Oferowane rozwiązanie musi wspierać cykliczne odtwarzanie środowisk wirtualnych. * Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji. * Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej. * Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej. * Rozwiązanie musi np. w formie email przesyłać informację na temat zakończonych zadań.   Zarządzenie oprogramowaniem do kopii zapasowej powinno być realizowane za pomocą przeglądarki internetowej z wykorzystaniem interfejsu graficznego. Rozwiązanie to musi:   * oferować dostęp administracyjny, * wskazywać liczbę danych objętych kopią zapasową, * zarządzać politykami kopii zapasowej, * monitorowanie wykonywanych czynności (wskazanie liczby kopii zapasowych, które obecnie są wykonywane, które są zakończone z sukcesem oraz ukończone niepowodzeniem), * system powinien umożliwiać nadawanie uprawnień i dostępów administratorom na podstawie definiowalnych ról na poziomie globalnym systemu   W przypadku, gdy został zaoferowany wirtualizator, który może pełnić rolę hypervisora dla maszyn wirtualnych oraz środowiska kubernetes dla kontenerów to rozwiązanie do kopii zapasowych musi zapewniać wyżej wymienione funkcjonalności, a także zapewniać w ramach kopii zapasowych kontenerów:   * Możliwość tworzenia pełnych kopii zapasowych maszyn kontenerowych * Kopii zapasowych w oparciu o minimum plikowy backupu, * Możliwość odtworzenia całej maszyny kontenerowej na środowisko wirtualizacji. * Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej. * Możliwość udostępnienia dysków maszyny kontenerowej w kopii zapasowej do innych systemów poprzez protokół iSCSI. * Możliwość pominięcia wybranych dysków maszyny kontenerowej z kopii zapasowej. * Możliwość automatycznego przypisywania polityk do maszyn kontenerowej w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki) * Możliwość automatycznego przypisywania polityk do maszyn kontenerowej w oparciu o przypisane w środowisku etykiety (ang. label). * Możliwość automatycznego wykonania polecenia na maszynie kontenerowej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej. * Rozwiązanie powinno umożliwiać zabezpieczenie bazy danych metadanych środowiska (etcd)   Rozwiązanie to powinno zostać dostarczone ze wszystkimi licencjami oraz wsparciem producenta do wykonania kopii zapasowej na okres minimum 60 miesięcy – nie jest akceptowane wsparcie typu „community support”, oferowane przez społeczność jego użytkowników lub wsparcie oferowane wyłącznie przez dostawcę. Po ustaniu licencji musi być zapewniona możliwość odtworzenia kopii zapasowej. | |

# Opis minimalnych parametrów technicznych dla 6 zapór sieciowych wraz z licencjami i oprogramowaniem:

|  |  |
| --- | --- |
| Architektura urządzenia | * Urządzenie będące dedykowaną platformą sprzętową producenta zapory sieciowej – nie dopuszcza się rozwiązań bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia, * Urządzenie musi pełnić rolę ściany ogniowej nowej generacji (next generation firewall) * Urządzenie musi wspierać mechanizm zapewniania wysokiej dostępności (HA) m.in. active/standby (active/passive) * Urządzenie musi posiadać uchwyty montażowe lub dedykowaną półkę do szafy RACK |
| Interfejsy sieciowe | * minimum 5 interfejsów obsługujących prędkość Gigabit Ethernet w standardzie RJ-45 * minimum 1 interfejs obsługujących prędkość Gigabit Ethernet w standardzie RJ-45 realizujący połączenie WAN , |
| Pozostałe interfejsy | * minimum jeden interfejs przeznaczony do zarządzania urządzeniem (tj. console port) * Minimum jeden port USB umożliwiający między innymi instalację oprogramowania z klucza (nośnika) USB * Minimum jedno gniazdo zasilania (wraz z oryginalnym zasilaczem), |
| Dysk twardy | * Minimum jeden dysk twardy SSD o pojemności minimum 128 GB |
| Realizowanie funkcji bezpieczeństwa | * Realizacja funkcji bezpieczeństwa modułu firewall (firewall throughput) na poziomie minimum 4.6 Gbps * Realizacja funkcji bezpieczeństwa ochrona przed zagrożeniami (threat prevention) na poziomie minimum 660 Mbps * Realizacja nie mniej niż 200 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. * Możliwość wykorzystania urządzenia do agregowania połączeń wdzwanianych (zestawienie połączenia VPN) dla minimum 80 klientów (wymagane dostarczenie jest niezbędnych licencji na połączenia VPN z urządzeń typu: laptop, tablet, telefon). Uwierzytelnienie klientów musi odbywać się w RADIUS/LDAP/AD., * Zapewnienie funkcjonalności dekrypcji SSL, * Możliwość realizowania bezpiecznego połączenia IPSec site-to-site, * Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) * Tworzone reguły firewall muszą uwzględniać minimum adresy IP, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń (logowanie). * Możliwość wykorzystania w polityce bezpieczeństwa m.in. kategorii URL, * Realizacja funkcjonalności typu wykrywania oraz zapobiegania włamaniom. W zależności od stworzonej polityki bezpieczeństwa funkcja IPS może być:   + w trybie detekcji,   + w trybie blokady, * System IPS musi mieć możliwość obsługi protokołu IPv6 * Zapora sieciowa musi mieć możliwość przesyłania logów do serwera syslog, * Możliwość realizacji funkcji bezpieczeństwa przed zagrożeniami (np. antywirus/ antymalware) * Możliwość uruchomienia urządzenia w trybie transparentnym, * Urządzenie obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP) * System filtracji zapewniający:   a. możliwość wykrywania aplikacji,  b. kategoryzację stron (URL),  c. bazę URL,   * Zapora musi umożliwiać wykrywanie złośliwego oprogramowania (malware) m.in.: sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze) |
| Zarządzanie | * Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania, * Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów, * Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP, * Element systemu pełniący funkcję Firewall musi umożliwiać skorzystanie z podstawowych narzędzi diagnostycznych, takich jak: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
| Licencje, oprogramowanie i gwarancje | Urządzenie powinno posiadać licencje na okres minimum 60 miesięcy od aktywacji:   * realizacji wszystkich modułów bezpieczeństwa, * zarządzania urządzeniem (w tym tworzenia reguł bezpieczeństwa), * licencje dostępowe dla klientów wdzwanianych, * dostępu do logów bezpieczeństwa   W przypadku, gdy wymagane jest dołączenie licencji lub oprogramowania w celu realizacji m.in. funkcjonalności dostępowych winno być dostarczone wraz z urządzeniem.  Rozwiązanie to powinno zostać dostarczone ze wszystkimi licencjami oraz wsparciem producenta na okres minimum 60 miesięcy – nie jest akceptowane wsparcie typu „community support”, oferowane przez społeczność jego użytkowników lub wsparcie oferowane wyłącznie przez dostawcę.  Gwarancja i wsparcie producenta na zapory sieciowe powinno wynosić minimum 60 miesięcy i polegać na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach gwarancji i wsparcia producent powinien zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |

# Opis minimalnych parametrów technicznych dla 12 przełączników sieciowych wraz z licencjami i oprogramowaniem:

|  |  |
| --- | --- |
| Obudowa i okablowanie | * Maksymalnie 1U z osprzętem niezbędnym do zainstalowania w szafie typu RACK, * komplet patchordów światłowodowych o długości minimum 5 metrów, * komplet okablowania do zapewnienia zasilania oraz kabel konsolowy, * komplet okablowania do pracy w stosie, |
| Interfejsy sieciowe | * minimum 24 interfejsów obsługujących prędkość Gigabit Ethernet w standardzie RJ-45, * minimum 4 interfejsy światłowodowe obsługujących prędkość minimum 10GbE wraz z odpowiednimi wkładkami, * minimium 2 interfejsy uplink 10GbE |
| Pozostałe interfejsy | * dostęp do interfejsu zarządczego po dedykowanym porcie konsolowym, * posiadać dwa redundantne zasilacze, |
| Realizowanie funkcje | * urządzenie powinno realizować przepustowość przełączania minimum 200 Gbps oraz minimum 100Gbps w ramach stosu, * realizować funkcjonalność przełącznika w warstwie drugiej i/lub warstwie trzeciej (w zależności od realizowanej konfiguracji), * Wielkość tabeli adresów MAC minimum 30 tys., * umożliwiać tworzenie minimum 1000 aktywnych wirtualnych podsieci (VLAN), * Obsługa Jumbo Frames, * Możliwość pracy w stosie (stack) dla minimum dwóch urządzeń * Obsługa protokołu NTP * Przełącznik zapewnia następujące mechanizmy:   + IEEE 802.1w Rapid Spanning Tree,   + IEEE 802.1s Multi-Instance Spanning Tree * Przełącznik zapewnia mechanizmy MACSec * Możliwość uruchomienia funkcji serwera DHCP * Przełącznik musi zapewnić mechanizm zapewaniających autentyczność uruchamianego oprogramowania * Przełącznik umożliwia obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego wykorzystując mechanizmy kopiowania ruchu np. traffic mirroring, SPAN, lub inny mechanizm, |
| Licencje, oprogramowanie i gwarancje | Urządzenie powinno zostać dostarczone z licencjami na okres minimum 60 miesięcy od aktywacji.  W przypadku, gdy wymagane jest dołączenie licencji lub oprogramowania w celu realizacji m.in. funkcjonalności dostępowych winno być dostarczone wraz z urządzeniem.  Gwarancja i wsparcie producenta na przełączniki sieciowe powinno wynosić minimum 60 miesięcy |

# Opis minimalnych parametrów technicznych dla 6 zestawów podtrzymywania energii:

|  |  |
| --- | --- |
| Specyfikacja ogólna | * Możliwość instalacji w szafie RACK (wraz z osprzętem), * Liczba akumulatorów minimum 16 (parametry znamionowe akumulatora 12V/ 9 Ah) – liczba akumulatorów może być osiągnięta za wykorzystaniem dedykowanego modułu rozszerzającego producenta urządzenia podtrzymującego zasilanie (UPS) wraz z możliwością instalacji w dedykowanej obudowie w szafie RACK * Masa urządzenia podtrzymywania zasilania powinna wynosić maksymalnie do 70 kg * Urządzenie musi posiadać minimum jeden wyświetlacz LCD, za którego można podejrzeć m.in. stan naładowania akumulatorów, moc elektryczną, konieczność wymiany akumulatorów i inne podstawowe parametry, * Urządzenie musi być wyposażone w minimum jeden port szeregowy, * Urządzenie musi być wyposażone w jedną kartę sieciową z interfejsem ethernetowym * Urządzenie musi być zasilane za pomocą napięcia w zakresie minimum 220V, * Urządzenie musi zapewniać sprawność minimum 91%, * Urządzenie musi zapewnić minimum:   + 7 portów z wykorzystaniem wtyku C13,   + 1 port z wykorzystaniem wtyku C19, |
| Prąd wyjściowy | * Moc wyjściowa powinna wynosić minimum 3000W * Zakres napięcia wyjściowego powinien wynosić minimum 220V * Prąd wyjściowy musi być prądem zmiennym |
| Licencje, oprogramowanie i gwarancje | W przypadku, gdy wymagane jest dołączenie licencji lub oprogramowania w celu realizacji funkcjonalności zarządzania urządzenie (np. zdalne monitorowanie) winno być dostarczone wraz z urządzeniem.  Gwarancja i wsparcie producenta na rozwiązanie musi wynosić minimum 60 miesięcy |

# Opis minimalnych parametrów technicznych dla 6 szaf teletechnicznych (szaf RACKowych):

**Dostawa 5 szaf teletechnicznych (szaf RACKowych) o parametrach:**

|  |  |
| --- | --- |
| Wymiary i wyposażenie | * Szerokość minimum 800 mm, * głębokość minimum 1200 mm, * Maksymalnie wysokość 42U 19” * Minimum 4x belka nośna, * Nośność minimum 1500 kg, * Wzmocniona półka pod instalację UPS, * Moduł wentylatorów sterowanych czujnikiem temperatury, * Przepusty kablowe szczotkowe, na zasilanie UPS i okablowanie LAN, * Klasa szczelności IP20 lub równoważna, * Niezbędne wyposażenie minimum półki, organizery, gniazdka zasilania/ listwy potrzebne do montażu sprzętu w ramach części I - V oraz UPS-a (3kVA) z modułem baterii, * Zostanie zapewniona dodatkowa półka do instalacji sprzętu serwerowego, |
| Gwarancja | Szafa powinna zostać dostarczona z kompletem wyposażenia gwarancją i wsparciem producenta/dostawcy na minimum 60 miesięcy |

**Dostawa 1 szafy teletechnicznej (szafy RACK) o parametrach:**

|  |  |
| --- | --- |
| Wymiary i wyposażenie | * Szerokość 800 mm * głębokość 1200 mm * Maksymalnie wysokość 42U 19” * Nośność 1500 kg * Wzmocniona półka pod instalację UPS * Moduł klimatyzacji sterowany czujnikiem temperatury * Przepusty kablowe na zasilanie UPS i okablowanie LAN * Klasa szczelności IP20 lub równoważna * Niezbędne wyposażenie minimum półki, organizery, gniazdka zasilania/ listwy potrzebne do montażu sprzętu w ramach części I - V oraz UPS-a (3kVA) z modułem baterii, * Zostanie zapewniona dodatkowa półka do instalacji sprzętu serwerowego, |
| Gwarancja | Szafa powinna zostać dostarczona z kompletem wyposażenia gwarancją i wsparciem producenta/dostawcy na minimum 60 miesięcy |

# Opis minimalnego zakresu dla instalacji i wsparcia:

* 1. **Dostawa i Instalacja urządzeń:**
     1. W ramach dostawy infrastruktury teleinformatycznej Wykonawca musi dostarczyć powyższy sprzęt do wskazanych poniżej jednostek organizacyjnych Województwa Małopolskiego. Dostawa i wdrożenie zostanie przeprowadzona w następujących lokalizacjach (wraz z podziałem na ilość dostarczonego sprzętu):

|  | Serwer konf. I z wirtalizatorem | Serwer konf. II z backupem | Zapora sieciowa | Przełącznik sieciowy | UPS | Szafa RACK |
| --- | --- | --- | --- | --- | --- | --- |
| Pedagogiczna Biblioteka Wojewódzka im. Hugona Kołłątaja w Krakowie | 1 | 1 | 1 | 2 | 1 | 1 |
| Pedagogiczna Biblioteka Wojewódzka w Nowym Sączu | 1 | 1 | 1 | 2 | 1 | 1 |
| Małopolski Zespół Jednostek Edukacyjnych w Krakowie\* | 1 | 1 | 1 | 2 | 1 | 1 |
| Biblioteka Pedagogiczna w Tarnowie | 1 | 1 | 1 | 2 | 1 | 1 |
| Zespół Jednostek Edukacyjnych Województwa Małopolskiego w Krakowie | 1 | 1 | 1 | 2 | 1 | 1 |
| Zespół Szkół Mistrzostwa Sportowego im. Stanisława Marusarza w Zakopanem | 1 | 1 | 1 | 2 | 1 | 1 |

Tabela 1 – Rozmieszczenie przedmiotu zamówienia w poszczególnych Jednostkach

Do Jednostki oznaczonego symbolem \* zostanie dostarczona szafa z modułem klimatyzacyjnym

* + 1. Wszystkie roboty towarzyszące Wykonawca wykona na swój koszt i odpowiedzialność. Wykonawca zapewni na własny koszt i ryzyko wszystkie niezbędne elementy zapewniające właściwy montaż, podłączenie i konfigurację niezbędne do ich prawidłowej pracy w tym m.in. mocowania, przewody, uchwyty, maskownice itp. zgodnie z najlepszymi praktykami oraz zaleceniami producenta danego rozwiązania. Wykonawca zapewni odpowiednie środki techniczne wraz z osprzętem w tym m.in. okablowanie sieciowe (minimum kable światłowodowe, kable miedziane) w celu podłączenia dostarczonej infrastruktury w ramach pkt I-VII. Jeśli wyniknie taka potrzeba, wykonawca zobowiązuje się do zapewnienia odpowiednich środków technicznych w celu dostosowania infrastruktury danej WSJO w tym wykonania drobnych prac budowlanych itp. Dotyczy to zapewnienia m.in. stabilnego dostępu do sieci energetycznej oraz instalacji systemów wyciągu powietrza lub wentylacji, które umożliwią odpowiednią cyrkulację powietrza i utrzymanie optymalnych warunków termicznych dla sprzętu, a także zapewnienia odpowiednich środków bezpieczeństwa i zapobiegawczych w przypadku zainstalowania klimatyzowanej szafy RACK. Wszystkie środki techniczne oraz prace integracyjne Wykonawca dostarczy oraz zainstaluje na własny koszt i przy użyciu własnych narzędzi.
    2. Wykonawca najpóźniej w dniu podpisania przez Strony protokołu odbioru dostawy, dostarczy dokument potwierdzający objęcie dostarczonych urządzeń gwarancją przez okres wskazany w umowie oraz dokument potwierdzający udzielenie licencji na oprogramowanie lub wskaże portal producenta poprzez który można zweryfikować wykupioną gwarancję na sprzęt i udzielone licencje na oprogramowanie.
    3. Dostarczony przez Wykonawcę sprzęt i oprogramowanie muszą być nowe i pochodzić z oficjalnego kanału dystrybucji a gwarancja, której sposób realizacji określono m.in. w projektowanych postanowieniach umowy musi obowiązywać na terenie Rzeczypospolitej Polskiej. Licencje upoważniają do aktywacji i korzystania z produktów minimum na terenie Rzeczypospolitej Polskiej. Licencje nie mogą być wcześniej aktywowane/używane.
    4. Wykonawca musi przeprowadzić prace konfiguracyjne polegających na zintegrowaniu dostarczonej infrastruktury z infrastrukturą już działającą w każdej z Jednostek WM. Konfiguracja i uruchomienie dostarczonej infrastruktury należy zintegrować odpowiednio do istniejącej już sieci m.in. LAN, WAN, energetycznej, a także wentylacyjnej. W przypadku konieczności wdrożenia nowych usług (takich jak np. serwer DHCP, serwer DNS, narzędzia do monitoringu) Wykonawca uruchomi takie usługi na dostarczonych licencjach systemu operacyjnego i dostarczonych urządzeniach.
    5. Wykonawca, zintegruje dostarczoną infrastrukturę w ramach pkt I-VII z infrastrukturą funkcjonującą już w poszczególnych Jednostkach Organizacyjnych Województwa Małopolskiego.
    6. Wykonawca musi przeprowadzić konfigurację urządzeń zapewniając rozwiązanie pozwalająca na zdalne wsparcie oraz diagnostykę usterek i awarii dla dostarczonych komponentów w ramach pkt I-VII. Dostęp do infrastruktury musi posiadać Wykonawca oraz Zamawiający, a także osoby wskazane na wniosek Zamawiającego. Na wniosek Zamawiającego, Wykonawca może odebrać uprawniania osobom wcześniej wskazanym przez Zamawiającego, a także zmodyfikować zakres jego uprawnień.
    7. Wykonawca musi przeprowadzić instalację i konfigurację oprogramowania systemowego dla wszystkich dostarczonych komponentów w ramach pkt I-VII.
    8. Wykonawca musi przeprowadzić hardering systemów operacyjnych i innych rozwiązań dostarczonych w ramach pkt I-VII.
    9. Wykonawca musi wdrożyć system kopii zapasowej, dokonać jego harderingu, przygotować minimum harmonogramy wykonywania kopii zapasowych zgodnie z najlepszymi praktykami.
    10. Wykonawca musi wdrożyć narzędzie monitorujące dostarczoną infrastrukturę, a także system EZD RP w trybie 24/7 wraz z możliwością wysyłania informacji minimum drogą mailową o wykrytej niedostępności lub anomalii (monitorowane będą m.in. dostępność, obciążenie, zajętość dysków twardych). Wykonawca będzie mógł monitorować dostarczoną infrastrukturę dowolnym przez siebie wybranym narzędziem (po akceptacji Zamawiającego) bazującym na licencji open source. Gwarancje i wsparcie na oprogramowanie do monitoringu może być świadczone przez Wykonawcę.
    11. Wykonawca zapewni minimum 6 certyfikatów SSL typu wildcard do zainstalowania systemu EZD RP ważnych przez cały okres świadczenia wsparcia technicznego do umowy. Certyfikaty SSL posłużą do zainstalowania systemu EZD RP w wersji testowej i produkcyjnej na dostarczonej infrastrukturze. Zamawiający dopuszcza aby certyfikaty były odnawiane co roku.
    12. Wykonawca po kompletnym wdrożeniu przeprowadzi prezentację oraz instruktaż dla Zamawiającego, a także osobom wskazanym przez Zamawiającego odnośnie procedur i dobrych praktyk, jakie muszą być zachowane przy obsłudze urządzeń podczas codziennej administracji przed podpisaniem protokołu odbioru będącego załącznikiem do umowy.
    13. Wykonawca zobowiązuje się, że gwarancja oraz wsparcie techniczne dla dostarczonego oprogramowania będącego przedmiotem dostawy, o którym mowa w pkt I-VII, nie będzie realizowane za pośrednictwem ogólnodostępnych forów internetowych, społeczności użytkowników (community) ani innych niekomercyjnych kanałów wsparcia. Gwarancja oraz wsparcie muszą być świadczone bezpośrednio przez producenta oprogramowania lub jego autoryzowanego partnera, w ramach oficjalnych, płatnych lub komercyjnych usług wsparcia, zapewniających określony poziom świadczeń (SLA), bez limitu liczby zgłoszeń oraz dostęp do aktualizacji i poprawek bezpieczeństwa.
  1. **Przeprowadzenie testów integracyjnych:**
     1. Wykonane prace integracyjne będą wymagały przeprowadzenia testów integracyjnych składających się z minimum:
* Testy łączności podstawowej
  + Ping i traceroute: Weryfikacja fizycznej łączności między urządzeniami za pomocą ping (sprawdzenie dostępności) i tracert/traceroute (analiza ścieżki pakietów).
  + Ręczne testy usług: Próby połączenia z serwerami za firewall-em przy użyciu protokołów takich jak HTTP/HTTPS, SSH lub RDP.
  + Testowanie dostępu/ dostępów pomiędzy urządzeniami dostarczonymi, a funkcjonującymi już w Jednostkach zależnych od Województwa Małopolskiego (w sposób dwukierunkowy inicjonowania połączenia),
* Konfiguracja firewalla poprzez minimum skanowanie portów do identyfikacji otwartych portów i usług
* Weryfikacja reguł:
  + Sprawdzenie, czy reguły dopuszczające daną komunikację sieciową zapewniają ruch sieciowy dla wymaganych protokołów (np. HTTP, DNS).
  + Potwierdzenie, że reguły blokujące nie nadpisują zezwoleń przez błędną kolejność.
* Testy awaryjne pozwalające na symulację przeciążeń sieciowych lub awarii połączeń, aby zweryfikować mechanizmy redundancji (wraz z testowaniem rozwiązania do podtrzymywania zasilania),
* Przeprowadzenie testów integracji z istniejącą infrastrukturą poprzez:
  + Kompatybilność protokołów - testy komunikacji między nowymi a istniejącymi urządzeniami pod kątem zgodności protokołów (np. TCP/IP, VLAN tagging).
  + Routing między podsieciami
  + Sprawdzenie, czy np. serwery mogą wymieniać dane z istniejącymi systemami (jeśli są obecne; np. dostęp do serwera aplikacyjnego, dostęp do serwera usługi katalogowej, itp.)
* Testy wdrożonej infrastruktury pod wirtualizację:
  + Zweryfikowanie możliwość tworzenia nowych maszyn wirtualnych (jeśli wirtualizator pozwala to tworzenie kontenerów) na wirtualizatorze oraz sprawdzenie poprawność ich konfiguracji zgodnie z założeniami.
  + Przeprowadzenie testów usuwania maszyn wirtualnych (jeśli wirtualizator pozwala to usuwanie kontenerów) i upewnienie się, że zasoby są zwalniane prawidłowo.
  + Sprawdzenie możliwość modyfikowania zasobów maszyn wirtualnych, takich jak pamięć RAM, dodanie dysku czy zmiany liczby procesorów.
  + Przetestowanie tworzenia migawkowych kopii stanu maszyny wirtualnej i kontenerów (jeśli wirtualizator zapewnia taką możliwość) oraz ich przywracanie do wcześniejszego stanu.
  + Zweryfikować poprawność działania operacji włączania i wyłączania maszyn wirtualnych i kontenerów (jeśli wirtualizator zapewnia taką możliwość).
* Testy wdrożonej infrastruktury przeznaczonej pod kopie zapasowe:
  + Przeprowadzenie testów tworzenia kopii zapasowych danych oraz ich odtworzenia, aby upewnić się, że proces backupu działa poprawnie.
  + Sprawdzić integralność danych po odtworzeniu oraz czas potrzebny na wykonanie zarówno kopii zapasowej, jak i jej przywrócenia.
  + Przetestować różne scenariusze, takie jak przywracanie pojedynczych plików czy całych maszyn wirtualnych.
* Testy włączenia i wyłączenia całego środowiska:
  + Przeprowadzić kontrolowane wyłączenie całej infrastruktury, w tym serwerów, przełączników, firewalli oraz pozostałych komponentów dostarczonych w ramach postępowania.
  + Sprawdzić, czy wszystkie systemy uruchamiają się poprawnie po ponownym włączeniu środowiska zgodnie z ustaloną sekwencją startową.
  + Zweryfikować dostępność usług po ponownym uruchomieniu oraz upewnić się, że dane są spójne i nie doszło do ich utraty.
  + Zweryfikować, czy system podtrzymywania energii działa prawidłowo.
* Testy dostępu zdalnego:
  + Należy przetestować dostęp zdalny do infrastruktury za pomocą rozwiązania VPN.
  + Zweryfikować wydajność dostępu zdalnego.
  + Upewnić się, że dostęp zdalny działa zarówno dla administratorów infrastruktury, jak i dla użytkowników końcowych.
  1. **Dokumentacja:**
     1. Wykonawca musi wykonać dokumentację techniczną zaoferowanych urządzeń w języku polskim, która będzie obejmować m.in.:
        1. Opis konfiguracji zainstalowanej infrastruktury wraz z ze schematem wykonanych połączeń,
        2. Najlepszymi praktykami do zarządzania i administracji,
        3. Kopie plików konfiguracyjnych,
        4. Opis sposobu aktualizacji, bezpiecznego włączania i wyłączania poszczególnych urządzeń,
        5. Bezpiecznym kanałem zostaną przekazane poświadczenia dostępowe do każdego komponentu w ramach dostarczonych urządzeń,
        6. Instrukcje dotyczące procedur odtworzeniowych i backupu,
        7. Dokumentację gwarancyjną i licencyjną.
  2. **Gwarancja na wykonane prace i wsparcie:**

4.1. Jeżeli ujawnią się wady lub usterki sprzętu w ramach przedmiotowego załącznika, których Wykonawca nie jest w stanie usunąć, Wykonawca zobowiązuje się do dostarczenia w terminie do 5 dni roboczych, liczonych od następnego dnia roboczego po wysłaniu przez Zamawiającego zgłoszenia gwarancyjnego za pomocą kanałów zgłoszeń określonych w § 4 ust 3 Umowy, nowego sprzętu wolnego od wad lub usterek o parametrach nie gorszych niż dostarczonego w ramach realizacji zamówienia.

4.2. Serwis przedmiotu zamówienia musi być realizowany przez Wykonawcę lub Producenta lub Autoryzowanego Partnera Serwisowego Producenta.

4.3. Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego Producenta sprzętu.

4.4. Każdorazowa naprawa gwarancyjna musi być uzgodniona z Zamawiającym w zakresie m.in.: terminu, godziny, miejsca i osoby serwisującej oraz zakresu prac. Po wykonanej naprawie gwarancyjnej Wykonawca sporządzi protokół z wykonanych prac, który zostanie przekazany do zatwierdzenia i podpisania przez pracownika Zamawiającego lub innej osoby wskazanej przez Zamawiającego. Podpisanie tego protokołu oznacza prawidłową naprawę gwarancyjną przedmiotu umowy i zamknięcie zgłoszenia gwarancyjnego.

4.5. Wykonawca, w ramach wsparcia zobowiązuje się do zapewnienia bezpłatnego wsparcia, bez limitu godzin na okres minimum 60 miesięcy, w ramach którego zapewni minimum:

* Gwarancję na wykonane prace integracyjne między dostarczoną infrastrukturą, a infrastrukturą funkcjonującą w Jednostce WM.
* Dokonanie zmian w konfiguracji na wniosek Zamawiającego w ramach dostarczonego sprzętu i zintegrowanego z infrastrukturą Jednostki WM lub na wniosek Jednostki WM z informacją do Zamawiającego.
* Przeprowadzenie lub wsparcie w przeprowadzeniu aktualizacji wszystkich lub pojedynczych komponentów dostarczonej infrastruktury (hardware oraz software).
* Wesprze w instalacji systemu EZD RP (wersja testowa i/ lub produkcyjna) w Jednostkach na dostarczonej i skonfigurowanej przez Wykonawcę infrastrukturze.
* W przypadku problemów z działaniem dostarczonej infrastruktury wykrytej przez Zamawiającego lub pracowników Jednostki, ujawniającej się nieprawidłowym działaniem aplikacji EZD RP lub innej zainstalowanej na dostarczonej infrastrukturze, Zamawiający dopuszcza możliwość odtworzenia środowiska aplikacji (jeśli nie ma potrzeby dostarczenia dodatkowej licencji do aplikacji, która ma zostać odtworzona) na środowisku Zamawiającego w celu wykrycia np. błędów i problemów ze stabilnością. Dostęp do infrastruktury Zamawiającego może być zrealizowany poprzez sesję współdzieloną bądź bezpośrednią sesję nagrywaną z wykorzystaniem sesji PAM. Dostęp bezpośredni wiąże się z dostarczeniem licencji typu CAL w celu uzyskania dostępu do środowiska zamawiającego.
* W przypadku wykrycia błędów związanych m.in. z aktualizacją systemu EZD RP, harderingu i innych czynności w Jednostkach spowodowaną m.in. błędnym działaniem dostarczonej infrastruktury, oprogramowania wirtualizacyjnego, a także innych komponentów Wykonawca musi wesprzeć Zamawiającego w rozwiązaniu problemów.
* Wykonawca będzie wspierał Zamawiającego w migracji danych pomiędzy systemami lub maszynami wirtualnymi dla systemu EZD RP na dostarczonej i skonfigurowanej przez Wykonawcę infrastrukturze.
* Modyfikację lub zmiany w działaniu dostarczonych systemów i aplikacji.
* Modyfikację harmonogramów kopii zapasowej lub sposobu jej wykonania.
* Wraz z Zamawiającym przeprowadzi testowe odtworzenie środowiska testowego lub produkcyjnego EZD RP lub innej maszyny wirtualnej dostarczonej w ramach postępowania minimum raz w roku i sporządzi odpowiednią notatkę z procedury odtworzeniowej.
* Będzie przekazywał wiedzę, która pozwoli na samodzielną obsługę utrzymania przez wskazane osoby w zespole Zamawiającego wdrożonej infrastruktury i oprogramowania.
* Będzie świadczył wsparcie techniczne i gwarancyjne, które będzie obejmowało obszar:
  + diagnostyki problemów użytkowania oprogramowania,
  + diagnostyki problemów użytkowania dostarczonego sprzętu,
  + rozwiązywania problemów z oprogramowaniem (bug fixes),
  + ochrony prawnej, chroniącej użytkownika przed naruszeniem praw stron trzecich.

4.6. Wykonawca zobowiązuje się do wykonania naprawy gwarancyjnej sprzętu na terenie Jednostek Województwa Małopolskiego, gdzie przedmiotowy sprzęt został zainstalowany w terminie do………….. dni roboczych (zgodnie z ofertą), w których zostanie usunięta usterka zgłoszona przez Zamawiającego, liczonych od przesłania Wykonawcy zgłoszenia gwarancyjnego . W przypadku braku możliwości naprawy ze względu na wady, które nie kwalifikują się do ich usunięcia, Wykonawca zobowiązuje się do dostarczenia w tym terminie sprzętu wolnego od wad o parametrach nie gorszych niż sprzęt wadliwy.

4.7. W ramach gwarancji na wykonane prace wdrożeniowe i instalacyjno-integracyjne Wykonawca zapewni wsparcie telefoniczne, zdalne oraz na miejscu u Zamawiającego oraz będzie realizował działania w zakresie:

4.7.1. Usuwania błędów w działaniu całego dostarczonego sprzętu oraz oprogramowania,

4.7.2. Wdrażanie lub wsparcie we wdrożeniu nowych wersji oprogramowania dla dostarczonego sprzętu oraz oprogramowania,

4.7.3. Przeprowadzania koniecznych zmian w konfiguracji wdrożonej infrastruktury (całego sprzętu i oprogramowania) zgodnie z wymaganiami na wniosek Zamawiającego,

4.7.4. Dodawanie lub modyfikowanie planu w systemie backupowym minimum nowych wersji systemu EZD RP (np. w przypadku aktualizacji systemu EZD RP),

4.7.5. Udzielania informacji dotyczących wdrożonego sprzętu oraz oprogramowania,

4.7.6. Przeprowadzenia koniecznych zmian w infrastrukturze Jednostki Województwa w ramach integracji istniejącej infrastruktury z infrastrukturą dostarczoną w ramach zamówienia.

4.8. Zamawiający będzie zgłaszał błędy, zakres zmian, zapytania dotyczące zakresu zawartego w pkt 2 oraz 4 pod wskazany przez Wykonawcę adres email …………………..……. lub nr telefonu …………………..……

4.9. Wykonawca zobowiązany jest do usunięcia błędów działania wdrożonej infrastruktury o których mowa w pkt 4.7.1 w terminie 2 dni roboczych od zgłoszenia.

4.10. Wykonawca zobowiązany jest do aktualizacji lub wsparcia Zamawiającego w aktualizacji wszystkich komponentów dostarczonej infrastruktury, o których mowa w pkt 4.7.2 w terminie 14 dni roboczych od zgłoszenia.

4.11. Wykonawca zobowiązany jest do przeprowadzania koniecznych zmian w konfiguracji w ramach dostarczonej infrastruktury, o których mowa w pkt 4.7.3 w terminie 2 dni roboczych od zgłoszenia.

4.12. Wykonawca zobowiązany jest do wprowadzenia koniecznych zmian w działaniu systemu backupowego na potrzeby poprawnego wykonywania kopii zapasowych dla systemu EZD RP, o którym mowa w pkt 4.7.4 w terminie 2 dni roboczych od zgłoszenia.

4.13. Wykonawca w okresie gwarancji będzie weryfikował minimum aktualizację, poprawki bezpieczeństwa oraz inne zalecenia Producenta zaoferowanego sprzętu i oprogramowania, a także wpływ na wdrożone środowisko oraz będzie rekomendował wdrożenie wszelkich poprawek i zmian.

4.14. Wykonawca zobowiązany jest do udzielania Zamawiającemu informacji dotyczących wdrożonego sprzętu oraz oprogramowania o których mowa w pkt 4.7.5 w terminie 3 dni roboczych od zgłoszenia.

4.15. Wykonawca zobowiązany jest do wykonania koniecznych zmian w działaniu infrastruktury Jednostki i dostarczonej infrastruktury w celu zapewniania dostępności środowiska (wdrożonego sprzętu oraz oprogramowania) o których mowa w pkt 4.7.6 w terminie 7 dni roboczych od zgłoszenia.

4.16. W przypadku wykrycia awarii krytycznej, Wykonawca zobowiązany jest do podjęcia działań naprawczych w terminie nie dłuższym niż 2 godziny od momentu otrzymania zgłoszenia awarii przekazanego kanałem komunikacji wskazanym w § 4 ust 3 Umowy.

Przez awarię krytyczną rozumie się sytuację polegającą na całkowitej niedostępności infrastruktury lub niedostępności któregoś z jej kluczowych elementów, skutkującą brakiem możliwości korzystania z aplikacji EZD RP w Jednostce.

4.17. W przypadku innych zgłoszeń Zamawiającego, Wykonawca musi zająć stanowisko do 10 dni roboczych od podjęcia informacji.

# Szkolenie

Dostawa minimum jednego certyfikowanego szkolenia w języku polskim dla trzech pracowników w zakresie administracji i zarządzania klastrem kontenerowym. Szkolenie ma na celu przekazanie uczestnikom wiedzy i umiejętności niezbędnych do efektywnego zarządzania środowiskiem kontenerowym Kubernetes, z uwzględnieniem najlepszych praktyk w zakresie bezpieczeństwa, monitoringu oraz skalowania aplikacji EZD RP w kontenerach.

Szkolenie będzie obejmowało następujący zakres:

1. Wprowadzenie do konteneryzacji
   1. Wprowadzenie podstawowych usług i pojęć kubernetes
   2. Wprowadzenie do architektury kubernetes
2. Tworzenie usług kontenerowych
   1. Provisioning usług kontenerowych
   2. Wykorzystanie kontenerów typu rootless
3. Zarządzanie kontenerami
   1. Zarządzanie cyklem życia kontenerów
   2. korzystanie z persistent storage przez kontenery
   3. dostęp do kontenerów
4. Zarządzanie obrazami kontenerów
   1. Dostęp do rejestrów
   2. Manipulacja kontenerami
   3. zarządzanie obrazami kontenerów
5. Tworzenie własnych obrazów kontenerów
   1. Projektowanie własnych obrazów kontenerów
   2. Budowanie własnych obrazów kontenerów z wykorzystaniem container files
6. Wdrażanie aplikacji kontenerowych
   1. Architektura oferowanego rozwiązania kubernetes
   2. tworzenie zasobów (resources) kubernetes
   3. tworzenie tras (routes)
   4. tworzenie aplikacji w trybie source-to-image
   5. tworzenie aplikacji z wykorzystaniem konsoli Web
   6. wdrażanie aplikacji kontenerowych na zaoferowanym rozwiązaniu kubernetes
7. Wdrażanie aplikacji wielokontenerowych
   1. Wymagania dla aplikacji wielokontenerowych
   2. Wdrażanie aplikacji wielokontenerowej na zaoferowanym rozwiązaniu
   3. Wdrażanie aplikacji wielokontenerowej na zaoferowanym rozwiązaniu z wykorzystaniem szablonów (template)
8. Rozwiązywanie problemów (troubleshooting) aplikacji kontenerowych
   1. Rozwiązaywanie problemów (Troubleshooting)
   2. Rozwiązywanie problemów (Troubleshooting) aplikacji kontenerowych

Szkolenia muszą być prowadzone w formie praktycznej a w ramach poszczególnych zagadnień muszą być dostępne praktyczne ćwiczenia pozwalające uczestnikom nabyć praktycznych umiejętności w zakresie omawianych zagadnień.

Szkolenie powinno trwać minimum 4 dni.

Każdy uczestnik powinien posiadać dostęp do środowiska laboratoryjnego (ćwiczeń).

Zaświadczeniem ukończenia szkolenia będzie przekazanie uczestnikom certyfikatu.

W ramach realizacji szkolenia Wykonawca lub centrum edukacyjne, które będzie odpowiedzialne za realizacje przedmiotowego szkolenia dostarczy materiały szkoleniowe oraz certyfikaty potwierdzające ukończenie kursu na własny koszt.