KONCEPCJA TECHNICZNA

(załącznik do Studium Wykonalności – dokumentacja techniczna projektu)

„LUBUSKIE CENTRUM KOMPETENCJI CYFROWYCH I USŁUG WSPÓLNYCH – DATA CENTER”

ZAŁĄCZNIK 4 – INFRASTRUKTURA TELETECHNICZNA

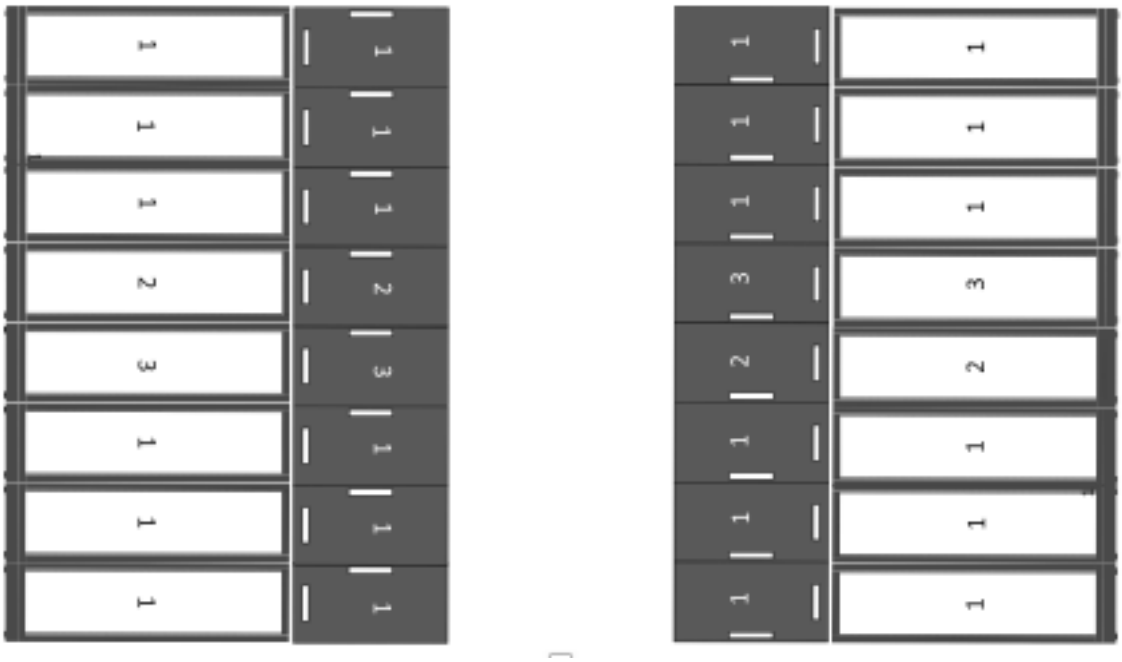
Comstar IT-CONSULTING
ul. Ułańska 7/82, 40-887, Katowice, Polska
NIP 6341201429
telefon +48 666209555
e-mail: lckciuw@icomstar.pl

Dokument opracowany przy współpracy z powołaną grupą roboczą w UMWL.

wersja 2.0, z dnia 5 grudnia 2021

1 INFRASTRUKTURA TELETECHNICZNA

Poniżej przedstawiony jest rzut (widok z góry) proponowanego rozmieszczenia szaf serwerowych w dedykowanym pomieszczeniu Data Center Lubuskiego Centrum Kompetencji Cyfrowych i Usług Wspólnych.



(1.Szafa serwerów – hostów; 2. Szafa rdzenia sieci; 3. Szafa macierzowa)

1.1 SZAFY DYSTRYBUCYJNE

Do zabudowy serwerowni wymagane będzie użycie szaf serwerowych 19” 42-47U 1000x1200 mm (szer. x gł.) Szafy muszą mieć nośność co najmniej 1000 kg. Szafy nie mogą się chwiać pod obciążeniem, dlatego muszą mieć wzmocnione narożniki, wykonane z jednego kawałka metalu, które łączą elementy ramy szafy. Poszczególne słupy i belki ramy nie mogą być skręcane śrubami bezpośrednio z sobą, gdyż nie zapewnia to ich wystarczającej stabilności względem siebie. Zwiększoną nośność należy zapewnić poprzez odpowiednią grubość blachy, co najmniej 2 mm, z której wykonany jest szkielet szafy. Szafa musi w standardzie zapewniać, zwiększoną pojemność, za pośrednictwem dodatkowych miejsc montażowych po bokach belek 19”, umieszczonych pionowo między belkami a ścianą boczna szafy. Oprócz podstawowych 42-47U musi zawierać dodatkowych 12U (6U przy przednich belkach 19”, 6U przy tylnych). Miejsca te będą mogły zostać wykorzystane do montażu listew zasilających i przełączników KVM. Drzwi szafy nie mogą się wyginać i falować przy otwieraniu, dlatego musza być wykonane z blachy co najmniej 2 mm grubości.

1.2 PRZEŁĄCZNIK LAN CORE

Przełącznik musi posiadać min. 24 porty o przepustowości 40Gbps na podłączenie przełączników w szafach serwerowych oraz min. dwa porty o przepustowości 100Gbps na połączenie z redundantnym przełącznikiem w drugim rzędzie szaf. Parametry minimalne przełączników sieciowych: Minimum 24 porty 40G, Minimum 2 porty 100Gb Przełącznik musi być wyposażony w kompatybilne z dostarczanymi urządzeniami wkładki w ilości odpowiadającej ilości portów Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management Port konsoli RS232 ze złączem DB9 lub RJ45 lub USB. Przepustowość minimum 480 Gb/s . Wydajność: minimum 285 Mp/s Przełączanie w warstwie 2 i 3 modelu OSI Wielkość bufora pakietów

(packet buffer): minimum 9MB Przełącznik musi wspierać obsługę IOT Minimum 2GB pamięci operacyjnej Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów) Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie.

1.3 PRZEŁĄCZNIK LAN

Parametry minimalne przełączników sieciowych: co najmniej 32 porty 10G/25G oraz co najmniej 4 porty 40Gb. Każdy przełącznik wyposażony w 4 wkładki 40Gb lub kable DAC niezbędne do podłączenia do infrastruktury. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az. Wsparcie dla funkcji Private VLAN lub równoważnego. Zainstalowane minimum 2 zasilacze.

1.4 PRZEŁĄCZNIK ZARZĄDZAJĄCY

Parametry minimalne przełączników sieciowych: Co najmniej 48 portów gigabitowych w standardzie 100/1000BaseT. Co najmniej 4 porty 10Gb SFP+. Każdy przełącznik wyposażony w 2 wkładki SFP+ 10Gb lub kable DAC niezbędne do podłączenia do infrastruktury. Przepustowość: minimum 128 Gb/s Wydajność: minimum 90 Mp/s 64byte Tablica adresów MAC o wielkości minimum 32000 pozycji. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az. Obsługa SNTPv4 lub NTP Wsparcie dla funkcji Private VLAN lub równoważnego. Zainstalowane minmum 2 zasilacze.

1.5 SERWER

Wysokości montażowej 2U , wyposażonych w 2 procesory po 16 rdzeni każdy , minimum 1024 GB RAM , wyposażonych w kartę sieciową 10/25GbE oraz w dwie karty Fibre Channel 32GB/s . Każdy serwerów musi posiadać redundantne zasilanie oraz wbudowany moduł zarządzania serwerem przez przeglądarkę. Serwery dostarczone zostaną z oprogramowanie do wirtualizacji posiadającym centralną konsolę zarzadzania w postaci appliance-u , oraz umożliwiającego utworzenie przełączników dystrybucyjnych pozwalających wykorzystanie protokołu LACP. Zostanie również dostarczone oprogramowanie umożliwiające instalacje nieograniczonej ilości instancji systemów operacyjnych, zgodnych z obecnie wykorzystywanymi systemami operacyjnymi poszczególnych jednostek. Minimalne parametry: Obudowa do instalacji w szafie Rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Procesor o architekturze x86, Ilość rdzeni dla procesora min. 15. Taktowanie procesora minimum 3,1 Ghz Obsługa minimum dwóch procesorów. Liczba zainstalowanych procesorów minimum 2. Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania minimum dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon). Zainstalowane minimum 1024GB pamięci RAM w kościach po 64GB. Minimum 24 sloty na pamięć, wsparcie pamięci typu RDIMM lub LRDIMM. Pamięć o częstotliwości minimum 3200MHz. Zabezpieczenie pamięci ECC, and Chipkill. Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. Port VGA. Zainstalowane dyski minimum 2 x 240 GB SSD Serwer musi posiadać co najmniej 8 zatok na dyski Hot-Swap, umożliwiających instalację dysków SATA/SAS – bez wymiany/dokładania jakichkolwiek elementów serwera. Możliwość instalacji dysków SED. Możliwość zastosowania w serwerze backplane'u umożliwiającego instalację zarówno dysków SATA/SAS jak i NVMe w tych samych zatokach z tym samym backplane zamiennie. Możliwość zainstalowania wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania klatek dyskowych serwera, możliwość konfiguracji jako RAID 0,1. Zainstalowany kontroler 12 Gb SAS/SATA z obsługą RAID 0, 1 Minimum dwa redundantne zasilacze o mocy minimum 1000W z certyfikatem minimum Platinum. Zainstalowane dwie karty FC 32 Gbps z wkładkami SWL Zainstalowana karta sieciowa dwuportowa - dwa porty 10/25Gb/s wraz z wkładkami LC jednomodowymi Minimum 3 gotowe do użytku port PCIe x8 oraz dedykowany, wewnętrzny slot dla kontrolera RAID. Możliwość

uzyskania min 3 slotów PCIe 3.0 x16 pełnej wysokości. Dodatkowe porty z przodu obudowy: 1x USB 3.0, 1x USB 2.0. Porty z tyłu obudowy: 2x USB 3.0, , 1x DB-15 Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania Monitoring statusu i zdrowia systemu

1.6 SERWEROWY SYSTEM OPERACYJNY

Musi być dostarczany do każdego z serwerów zgodnie z wymogami licencjonowania, wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play) graficzny interfejs użytkownika obsługa systemów wieloprocesorowych, obsługa platform sprzętowych x86, x64, możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowego programowania: usługi sieciowe DNS i DHCP, usługi katalogowe pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), zdalna dystrybucja oprogramowania na stacje robocze, praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, PKI (Centrum Certyfikatów, obsługa klucza publicznego i prywatnego), szyfrowanie plików i folderów, szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), możliwość rozłożenia obciążenia serwerów, serwis udostępniania stron WWW, serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management), wsparcie dla protokołu IP w wersji 6 (IPv6). Możliwość tworzenie serwerów wirtualnych, oprogramowanie wspierające tworzenie serwerów wirtualnych musi spełniać następujące wymagania funkcjonalne: warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych licencja musi umożliwiać zmianę wersji oprogramowania na niższą (downgrade) rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze, możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-4 wirtualnych kart sieciowych, możliwość przydzielania większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji, możliwość udostępniania maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy, konsola graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności, możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach, możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją danymi, możliwość integracji z usługami katalogowymi Microsoft Active Directory. Mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn obsługa przełączania ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek. możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, mechanizm wysokiej dostępności HA, w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym, funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej, pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia w razie awarii karty sieciowej, wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.

Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. 50 licencji dostępowych na urządzenie dla każdego z dostarczanych serwerów, umożliwiających zarządzanie urządzeniami z poziomu serwera AD za pośrednictwem usługi Active Directory.

1.7 LICENCJA SERWERA FIZYCZNEGO

Licencja dla każdego serwera fizycznego na minimum 2 procesory ze wsparciem technicznym oraz gwarancją utrzymania aktualnej wersji przez okres min. 3 lata. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Należy dostarczyć 1 licencję Virtual Appliance na wszystkie dostarczane serwery. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w

obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. Musi istnieć możliwość skonfigurowania przełącznika dystrybucyjnego i wykorzystania protokołu LACP/ Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

1.8 MACIERZ

Możliwość zainstalowania w standardowej szafie RACK 19”. Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości upakowania - co najmniej 24 dyski na 2U wysokości dla dysków 2,5 cala oraz półki dyskowe zawierające co najmniej 12 dysków 3,5 cala na wysokości 2U. Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości umożliwiające upakowanie co najmniej 92 dysków. Urządzenie musi umożliwiać zarządzanie za pomocą interfejsu Ethernet. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. Interfejs zarządzający GUI, CLI, oraz zapewnienie możliwości tworzenia skryptów użytkownika. Wymagane jest nie mniej niż 4 porty 10Gb Ethernet Base-T oraz 8 portów 32Gb FC wyposażonych we wkładki SFP+ 32Gb SWL. Musi obsługiwać dyski SAS jak również musi obsługiwać dyski SSD oraz musi obsługiwać dyski NVMe, musi obsługiwać, co najmniej 500 dysków na parę kontrolerów z zastosowaniem dodatkowych półek. Macierz musi umożliwiać rozbudowę o pojedyncze dyski fizyczne i pojedyncze półki rozszerzeń. musi umożliwiać konfigurację, która w jednym rozwiązaniu łączyć będzie półki rozszerzeń na dyski 2,5” z półkami na dyski 3,5”. Macierz dyskowa musi być wyposażona w minimum: 52 dyski NVMe o pojemności 19.2TB Macierz musi zapewnić możliwość wymiany uszkodzonych dysków podczas pracy systemu (Hot-Swap). Macierz musi być umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczego dysku oraz odporność na awarię dwóch dysków. Przestrzeń zapasowa powinna być realizowana za pomocą przestrzeni zapasowej rozmieszczonej na wszystkich dyskach w ramach grupy RAID lub w formie dysku nadmiarowego. Macierz musi być wyposażona w minimum 64GB pamięci Cache. Macierz musi umożliwiać rozbudowę pamięci cache do 128GB w ramach klastra macierzy zarządzanego z jednego interfejsu GUI, CLI. Wszystkie krytyczne komponenty urządzenia takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą być wymienialne w trakcie pracy macierzy. Urządzenie musi cechować brak pojedynczego punktu awarii. Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap. Wentylatory typu Hot-Swap. Wbudowane co najmniej dwa kontrolery RAID. Urządzenie musi posiadać pamięć typu Flash dla zapisu danych z pamięci cache na wypadek zaniku zasilania oraz system podtrzymania zasilania pozwalający na zapis danych z cache do pamięci typu Flash Musi istnieć funkcjonalność Cache dla procesu odczytu.

1.9 PRZEŁĄCZNIK SAN FC

Wymagana jest instalacja czterech przełączników SAN. Każdy Przełącznik FC musi być wykonany w technologii FC 64 Gb/s i posiadać możliwość pracy portów FC z prędkościami min 64, 32, 16 z funkcją auto negocjacji prędkości.

Każdy Przełącznik FC musi posiadać minimum 56 slotów na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla 24 portów FC przełącznika. Każdy przełącznik musi być dostarczony wraz z minimum 24 modułami SFP FC 32 każdy Gb/s SW oraz dwoma modułami SFP+ 64 Gb/s SWL Rodzaj obsługiwanych portów: min E_Port, F_Port;. Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w szafie 19". Przełącznik FC musi posiadać nadmiarowe wentylatory N+1 Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking" uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. Urządzenie musi umożliwiać połączenie przełączników w jeden „fabric" (funkcjonalność ISL), dostarczyć licencje, jeśli wymagane. Możliwość wymiany w trybie „na gorąco": minimum w odniesieniu do modułów portów Fibre Channel (SFP). Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. Szyny do montażu w szafie rack. Zainstalowane minimum 2 zasilacze.

1.10 KONSOLA KVM

Wysuwana klawiatura z integrowana z monitorem o przekątnej minimum 18'' i rozdzielczości minimalnej 1366x768 pikseli. Układ klawiatury QWERTY Język klawiatury US International, Wbudowany w klawiaturę Touchpad Po złożeniu obudowa o wysokości maksymalnie 1U Możliwość podłączenia min. 16 serwerów. W zestawie muszą być dostarczone kable do podłączenia 16 serwerów na konsolę Obsługa portów VGA oraz 2 portów USB. Poprzez klawisze na klawiaturze lub menu OSD Wbudowany moduł do zdalnej obsługi konsoli.

1.11 MACIERZ Z ROZWIĄZANIEM DO BACKUP

System musi składać się ze sprzętu (macierzy dyskowej) oraz oprogramowania. Macierz musi składać się z półki dyskowej (JBOD), obsługującej min. 64 dyski HDD SATA/SAS 3,5" oraz serwera. Półka dyskowa musi być połączona z serwerem za pomocą kontrolera SAS. Półka dyskowa musi być wypełniona dyskami HDD o pojemności min. 10 TB i prędkości min 7200rpm. Minimalne parametry serwera sterującego półką dyskową: Procesor min. 8 rdzeni i taktowaniu min. 3 GHZ Pamięć RAM min 128GB Kontroler SAS Karta sieciowa dwuportowa o prędkości 10/25Gb/s LC Redundantne zasilanie Obudowa max. 2U. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner:https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.

1.12 UTM

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall. Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii

W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
System realizujący funkcję Firewall musi dysponować minimum: 16 portami 10 Gigabit Ethernet RJ-45.16 portami 10 sfp+/25 GE SFP28,2 gniazdami SFP+ 10 Gbps. 4 gniazdami QSFP28 100 Gbps/40 GE QSFP+ System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. System musi posiadać 2 gniazda zasilania AC. W zakresie Firewall'a obsługa nie mniej niż 24 mln. jednoczesnych połączeń oraz 1 mln. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 198 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 64 Gbps. Wydajność szyfrowania IPSec VPN nie mniej niż 55 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 24 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 17 Gbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 20 Gbps. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. Kontrola Aplikacji. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. Ochrona przed atakami - Intrusion Prevention System. Kontrola stron WWW. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. Zarządzanie pasmem (QoS, Traffic shaping). Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

1.13 BIBLIOTEKA TAŚMOWA

Obudowa biblioteki przystosowana do montażu w standardowej szafie rack 19''. Maksymalna wysokość biblioteki podstawowej 3U. Cała oferowana biblioteka wyposażona w cztery napędy LTO nie może przekraczać wysokości 6 U. Biblioteka taśmowa musi być wyposażona w co najmniej dwa napędy taśmowe typu LTO8 o natywnej przepustowości 300 MB/s oraz interfejsem FC min. 8 Gbit/s. Każdy napęd taśmowy musi z kompresją: odczytywać i zapisywać taśmy typu LTO8 oraz LTO7. Wszystkie sloty znajdujące się w bibliotece muszą być aktywne – jeżeli do aktywacji wymagana jest licencja musi być dostarczona. Biblioteka musi udostępniać dla serwerów nie mniej niż 80 sztuk slotów na taśmy typu LTO. Biblioteka musi mieć funkcjonalność partycjonowania na co najmniej cztery niezależne biblioteki logiczne. Musi być możliwość zdefiniowania przez operatora od 1 do co najmniej 70 wirtualnych slotów na taśmy do każdej biblioteki logicznej (partycji). Biblioteka musi być wyposażona w czytnik kodów kreskowych umożliwiający automatyczne rozpoznawanie i inwentaryzację taśm załadowanych do biblioteki. Biblioteka musi być wyposażona w pamięć przechowującą stan inwentaryzacji w formie listy etykiet taśm (VOLSER). Biblioteka musi być wyposażona w robota obsługującego automatyczne załadowanie i rozładowanie taśm pomiędzy slotami, portami wejścia/wyjścia i napędami taśmowymi. Możliwość monitorowania stanu biblioteki i napędów co najmniej dwiema niezależnymi metodami: przez panel sterowania umieszczony na frontowej obudowie biblioteki oraz GUI. Bezpieczeństwo dostępu musi być chronione co najmniej poprzez nazwę użytkownika i pin/hasło oraz trzy poziomy użytkowników: administrator, operator, serwis.

1.14 ROZWIĄZANIE CYBERBEZPIECZEŃSTWA JEDNOSTEK UMWL W CHMURZE PRYWATNEJ LCKIUW

W ramach usług wspierających realizacje e-usług publicznych jak również na potrzeby obsługi administracji UMWL oraz zainteresowanych jednostek podległych oraz jednostek samorządowych, planuje się uruchomić usługę zabezpieczeń zasobów sieci jednostek klienta, komputerów w tych jednostkach (endpoint protection) oraz poczty elektronicznej.

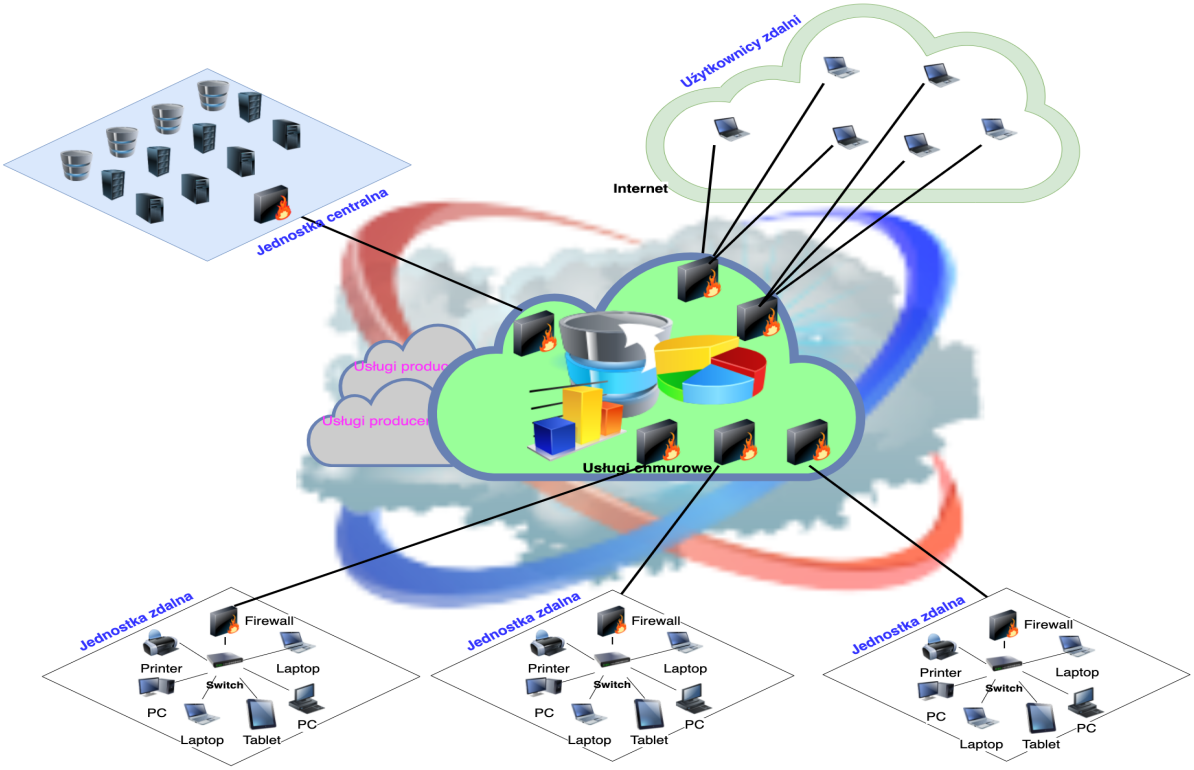
Zabezpieczenie komputerów odbędzie się przy pomocy systemów klasy endpoint protection i pozwoli na zaawansowaną ochronę urządzeń końcowych przed wszelkimi atakami znanymi bądź nieznanymi, w tym złośliwego oprogramowania, bezplikowymi, ransomware oraz działalnością oprogramowania niepożądanego (PuP). Umożliwi zapobieganie potencjalnym zagrożeniom „dnia zerowego" na urządzeniach, poprzez analizę zarówno bezpośrednio na urządzeniu jak i w środowisku chmurowym (na terenie Unii Europejskiej) w trybie online oraz tworzenie nowych zasad bezpieczeństwa dla ochrony całego środowiska. Zapewni rozpoznawanie technik ataku złośliwego oprogramowania na poziomie urządzenia. Zmniejszy powierzchnie ataku poprzez szczegółowe zarządzanie aplikacjami uruchamianymi na zabezpieczonych komputerach - kontrolę ich wersji i dystrybucji wśród wszystkich zasobów komputerowych. Umożliwi również aktywną ochronę urządzeń nie podłączonych do Internetu i bez ochrony sieciowej. Jest to element niezbędny w przypadku, kiedy złośliwe oprogramowanie lub exploit zostaną dostarczone innymi metodami niż przez sieć (np. USB, bluetooth) i/lub urządzenie jest odcięte od sieci. Zwiększy odporności urządzeń końcowych (stacji roboczych, serwerów) na ataki, poprzez szczegółową kontrolę istniejących w zasobach organizacji podatności ich systemów operacyjnych i wykorzystywanych aplikacji. Zapewni pełną widoczność aktywności użytkowników, plików, procesów uznanych za podejrzane. Zapewnione będzie wdrożenie obsługi białych list aplikacji niepożądanych/zabronionych a jednak dopuszczonych do użytkowania (whitelistening). Umożliwi się ochronę przed niepożądanymi próbami uzyskania dostępu do stacji roboczych, urządzeń mobilnych oraz serwerów również poprzez audytowanie logowania do stacji roboczych/serwerów użytkowników z uprawnieniami administratora oraz monitorowanie polityki zmiany haseł. Z punktu widzenia obsługi użytkowników komputerów ważne jest iż wdrożone rozwiązanie nie będzie wymagało jakiejkolwiek rozbudowy infrastruktury klienta. Konieczne będzie jedynie zainstalowanie oprogramowania klienckiego (agenta), który będzie działać w sposób niezauważalny dla użytkownika komputera, nie będzie wymagał dodatkowej konfiguracji czy dostrajania po instalacji. Praca agenta nie będzie również miał wpływu na wydajność działania oprogramowania używanego przez klienta.

Zabezpieczenie sieci jednostek odległych i Data Center odbędzie się poprzez wdrożenie infrastruktury bezpiecznej bramy do Internetu dla pracowników każdej jednostki korzystającej z bezpieczeństwa LCKCiUW oraz ustalenie polityk dostępu do przeglądania zasobów Internetu, w celu uniknięcia dostępu do niebezpiecznych witryn będących częściami ataków (np. phishingowych, dystrybuujących i zawierających złośliwy kod czy oprogramowanie, itp.). Wykorzystana zostanie funkcjonalność uaktualnianej w trybie ciągłym bazy kategorii URL, wspieranej przez wiodących dostawców rozwiązań cyberbezpieczeństwa. Pozwoli to na zmniejszenie liczby incydentów bezpieczeństwa przed ich zaistnieniem w infrastrukturze chronionych jednostek. Możliwe będzie również wprowadzenie limitowania dostępu do zasobów bezpiecznych, lecz niepożądanych przez pracodawcę (media społecznościowe, portale aukcyjne, gry online, itp.). Świadczone przez LCKCiUW usługa umożliwi inspekcję ruchu pod względem obecności exploitów, złośliwego oprogramowania, złośliwych URL, a także zawartości niebezpiecznej lub z ograniczeniami jak również analizę zagrożeń typu „sandbox" do kontroli plików, która automatycznie stworzy nowe zasady ochrony. Możliwe będzie stworzenie mechanizmów skutecznego i automatycznego rozpoznawania nietypowej aktywności w sieci, zapewniającego dokładne informacje, które pozwalają na szybkie oszacowanie potencjalnego zagrożenia, jego izolację i usunięcie zanim zdąży ono wyrządzić szkody. Uruchomione zostaną polityki limitujące typy danych (plików) mogących podlegać wymianie pomiędzy jednostkami (np. dozwolone będą tylko pliki biurowe i bazy danych, ale nie pliki wykonywalne) z możliwością tworzenia wyjątków. Uruchomiona zostanie także usługa inspekcji przesyłanych danych (plików) na urządzeniach w trakcie ich transmisji, a w razie potrzeby w chmurze producenta zlokalizowanej na terenie Unii Europejskiej. Umożliwi to również wdrożenie bezpiecznej pracy zdalnej dla pracowników przebywających poza UMWL/

jednostkami podległymi lub jednostkami samorządowymi. W zależności od rzeczywistych potrzeb, w jednostkach odległych zostanie zainstalowany (lub wykorzystany istniejący) firewall nowej generacji (NGFW) chroniący całe sieci tych jednostek lub oprogramowanie chroniące jedynie komputery (agent VPN) Ważnym z punktu bezpieczeństwa danych jest fakt iż transmisja danych pomiędzy jednostkami będzie prowadzona jedynie w oparciu o bezpieczne szyfrowane tunele IPSec przy wykorzystaniu mocnych metod kryptograficznych;

Ze względu na fakt iż najbardziej rozpowszechnionym wektorem ataku jest nadal poczta elektroniczna, w obszarze cyberbezpieczeństwa szczególny nacisk zostanie postawiony na ochronę poczty, zaproponuje się UMWL, jednostką podległym oraz jednostką samorządowym przeniesienie serwerów pocztowych z innych hosingów lub swoich serwerów na serwery LCKCiUW. Zostaną wdrożone dedykowane systemy chroniące infrastrukturę poczty klienta zanim potencjalne zagrożenie do niej dotrze. Mechanizmy ochrony przed zagrożeniami związanymi z phishingiem, złośliwym oprogramowaniem, spamem oraz innymi formami niewłaściwych lub niebezpiecznych treści oraz zaawansowana ochrona przed złośliwymi adresami URL i załącznikami. Wdrożone usługi zapewnią bezpieczeństwo wrażliwych danych opuszczających organizację jak również filtrowanie treści oraz przesyłania nielegalnych obrazów z załączników.

W kolejnym etapie możliwe będzie stworzone zostanie Security Operation Center (Centrum zarządzania zagrożeniami) czyli specjalnie utworzonego działu bezpieczeństwa składającego się z ekspertów zajmujących się analizą incydentów oraz naruszeń bezpieczeństwa IT w czasie rzeczywistych, zespół ten byłby dedykowany do wspierania procesów i technologii zawartych w usłudze, do dyspozycji każdego dnia roboczego (8/5). Stworzenie takiego zespołu wymaga analizy finansowej oraz określonej grupy złożonej z chętnych jednostek podległych Urzędowi Marszałkowskiemu jak i jednostek samorządu terytorialnego. Powstanie takiego zespołu umożliwiłoby świadczenie usług również na zewnątrz do obywateli i przedsiębiorców, komercyjnie po zakończeniu okresu trwałości projektu lub nawet w okresie trwałości w przypadku, gdy zysk pokrywałby jedynie koszty związane z utrzymaniem usługi.



„Lubuskie Centrum Kompetencji Cyfrowych i Usług Wspólnych – Data Center" współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Urzędu Marszałkowskiego w ramach Regionalnego Programu Operacyjnego Województwa Lubuskiego na lata 2014-2020, oś priorytetowa 2 rozwój cyfrowy; działanie 2.1 rozwój społeczeństwa informacyjnego.

2 SPECJALISTYCZNE URZĄDZENIA IT NA POTRZEBY E-USŁUG

W poniższym rozdziale opisano sprzęt komputerowy, który zostanie zainstalowany w siedzibie Departamentu Geodezji, Gospodarki Nieruchomościami, i Planowania Przestrzennego oraz Zarządzie Dróg Wojewódzkich. Opisywany sprzęt komputerowy będzie wykorzystywany w procesach związanych ze świadczeniem e-usług. Urządzenia muszą być fabrycznie nowe i spełniać niżej podane parametry techniczne (minimalne). Beneficjent dopuszcza zaoferowanie sprzętu o parametrach lepszych od wymagań minimalnych.

2.1.1 E-USŁUGI W DEPARTAMENT GEODEZJI, GOSPODARKI NIERUCHOMOŚCIAMI I PLANOWANIA PRZESTRZENNEGO

W ramach zakresu realizacji projektu e-usług zostaną dostarczone, zainstalowane, skonfigurowane i uruchomione następujące urządzenia:

1. Stacja robocza stacjonarna – 9 sztuk
2. Monitor – 9 sztuk
3. Wyposażenie dodatkowe – 9 sztuk
4. Specjalistyczne oprogramowanie – 9 sztuk
5. Notebook – 9 sztuk

2.1.1.1 STACJA ROBOCZA STACJONARNA

CPU Min 18 rdzeniowy Zaoferowany procesor przynajmniej raz musi znajdować się na stronie internetowej https://www.cpubenchmark.net/desktop.html i na przedstawionym wykresie PassMark - CPU Mark, uzyskał ranking co najmniej 25000 (25,000) punktów.
Pamięć RAM: min. 128 GB DDR4; obsługiwane min. 256 GB; zainstalowana jako 2 x 64 GB;min 4 porty pamięci;
Karta graficzna: Karta graficzna do zastosowań 2D/3D, min. 16GB 256-bit GDDR6; maksymalna rozdzielczość – min. UHD 3840x2160 pikseli @120Hz;Min. 2x złącze DisplayPort; Wspierany standard DisplayPort min. 1.4 Wspierany standard HDR (High Dynamic Range);Wspierany standard kompresji DSC (Display Stream Compression) min. 1.2;
Dyski HDD: minimum 2 x 2TB GB SSD A.

2.1.1.2 MONITOR

Monitor z wbudowaną kamerką szerokokątną. Wielkość ekranu: 32 do 49 cala. Rozdzielczość: Min UHD 3840 x 2160 pikseli @ 144Hz. Złącza Minimum 1 x Display Port, standard DP min. 1.4; Wbudowany HUB USB z minimum 2 portami USB wraz z przewodem obsługującym standard min. USB 3.1; Jasność (typ.): Minimum 250 cd/m2, Kontrast (typ.): 1000:1

2.1.1.3 WYPOSAŻENIE DODATKOWE

Ergonomiczna bezprzewodowa klawiatura oraz mysz. Typ: Multimedialna, łączność bezprzewodowa, klawisze numeryczne, podpórka pod nadgarstki. Mysz o rozdzielczości minimum 1000 DPI, w technologii BlueTrack

2.1.1.4 SPECJALISTYCZNE OPROGRAMOWANIE

ArcGIS Enterprise Advanced

2.1.1.5 NOTEBOOK

Typ „yoga”, pamięć RAM: 8 GB (DDR4, 2400MHz), maksymalna obsługiwana ilość pamięci RAM 64 GB, liczba gniazd pamięci (ogółem / wolne): 2/1, dysk SSD M.2 PCIe: 500 GB, przekątna ekranu: 14,0" – 15,6”, rozdzielczość ekranu: 1920 x 1080 (FullHD), karta graficzna: min AMD Radeon™ Vega 3, wbudowane głośniki stereo oraz mikrofon i kamera, łączność Wi-Fi, moduł bluetooth, złącza: USB 3.2 Gen. 1 - 2 szt., USB Typu-C - 1 szt., HDMI - 1

szt., czytnik kart pamięci SD - 1 szt, wyjście słuchawkowe/wejście mikrofonowe - 1 szt, system operacyjny: Microsoft Windows 10 PRO (wersja 64-bitowa), dodatkowe oprogramowanie: partycja recovery (opcja przywrócenia systemu z dysku), Microsoft Office 2019.

2.1.2 ZARZĄD DRÓG WOJEWÓDZKICH W ZIELONEJ GÓRZE

W ramach zakresu realizacji projektu e-usług zostaną dostarczone, zainstalowane, skonfigurowane i uruchomione następujące urządzenia:

1. Stacje robocze mobilne – 21 sztuk
2. Stacja robocza stacjonarna – 1 sztuka
3. Monitor 24'' – 42 sztuki
4. Monitor 65'' – 4 sztuki
5. Tablet RTK z anteną oraz dodatkową tyczką– 28 sztuk
6. Kamery obrotowe – 10 sztuk
7. Kamery ANPR – 10 sztuk
8. Urządzenia transmisji danych z kartami SIM i prywatnym APN – 10 sztuk

2.1.2.1 STACJA ROBOCZA MOBILNA

Komputer przenośny typu notebook z ekranem o przekątnej minimum 17" o rozdzielczości minimum 1920x1080 px (FullHD), przeciwodblaskowy, podświetlenie LED. Procesor: Architektura zgodna z x86, wielordzeniowy, wykonany w technologii mobilnej, osiągający w teście Passmark 8.0 CPU Mark nie mniej niż 9500 punktów. Pamięć RAM: 16 GB, DDR4, Dyski: 500GB w technologii SSD. Karta graficzna: Grafika musi osiągać w teście Passmark 8.0 G3D Mark minimum 2100 punktów (do weryfikacji podczas ogłaszania postępowania), minimum 2 GB własnej (niewspółdzielonej pamięci RAM). Multimedia: Karta dźwiękowa zgodna z HD Audio 24-bit, wbudowane głośniki stereo o mocy minimum 2x1 W. Bateria i zasilacz: Umożliwiająca szybkie naładowanie do poziomu 80% w czasie 60 minut i do poziomu 100% w czasie 120 minut. System operacyjny: System operacyjny 64-bit, Klucz zaszyty trwale w BIOS na etapie produkcji komputera I automatycznie pobierany przez Instalowane oprogramowanie.

2.1.2.2 STACJA ROBOCZA STACJONARNA

Typ: Komputer stacjonarny. Pamięć RAM: 32 GB (2x16384 MB) DDR4 możliwość rozbudowy do nie mniej niż 64 GB, dwa sloty wolne. Karta graficzna: Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem dla HDMI v1.4, ze sprzętowym wsparciem dla kodowania H.264 oraz MPEG2, DirectX 11.1, OpenGL 4.5, OpenCL 1.2, Shader 5 posiadająca min. 24 GEU (Graphics Execution Units) o maksymalnej rozdzielczości nie mniejszej niż: 4096x2304 px @ 60 Hz (cyfrowo).Wymagane min. 3 wyjścia cyfrowe – DisplayPort, DVI lub HDMI w dowolnej konfiguracji ilościowej pod warunkiem dostarczenia adapterów umożliwiających jednoczesne podłączenie min. 2 monitorów w tym jednego ze złączem DVI. Wymagane nie mniej niż 2 wyjścia cyfrowe – DisplayPort, DVI lub HDMI w dowolnej konfiguracji ilościowej pod warunkiem dostarczenia adapterów umożliwiających jednoczesne podłączenie nie mniej niż 2 monitorów w tym jednego ze złączem DVI. Dyski HDD: 1 x 500 GB SSD M.2 NVMe, 1 x 1 TB SATA. Obudowa: Typu MiniTower z obsługą kart PCI Express wyłącznie o pełnym profilu, wyposażona w nie mniej niż 4 kieszenie: 2 szt. 5,25" zewnętrzne (dopuszcza się wnęki 1x 5,25" pełnych wymiarów i 1x 5,25" slim na napęd optyczny) i 2 szt. 3,5" lub 2,5" wewnętrzne. Zasilacz o mocy (ciągłej) minimalnej 250W ale nie więcej niż 300W pracujący w sieci 230 V 50/60 Hz prądu zmiennego i sprawności nie mniej niż 92% przy 50% obciążeniu zasilacza. Komputer wyposażony na panelu przednim zdejmowany bez użycia narzędzi filtr powietrza chroniący wnętrze komputera przed kurzem, pyłem itp. Wymagania dodatkowe: Preinstalowany, 64-bitowy system operacyjny, w wersji PL, niewymagający podawania klucza licencyjnego podczas instalacji. Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE. Płyta główna z wbudowanymi: 1

niezajętym złączem PCI Express x16 3 generacji, 1 niezajęte złącze PCI Express x4; 1 niezajętym złączem PCI Express x1; 4 złącza DIMM z obsługą do 64 GB DDR4 pamięci RAM, nie mniej niż 4 złącza SATA w tym 3 szt. SATA 3.0, 1 złącze M.2 dedykowane do PCI-Express 3.0 x4; zintegrowany z płytą główną kontroler RAID 0 i RAID 1. Klawiatura USB w układzie US. Mysz optyczna USB z rolką (scroll). Nagrywarka DVD +/-RW. Dołączony nośnik ze sterownikami. Komplet sterowników umożliwiający instalację systemu operacyjnego

2.1.2.3 MONITOR

Wielkość ekranu Minimum 24, panoramiczny. Rozdzielczość Minimum 1920x1080. Czas reakcji matrycy Maksymalnie 6ms (gray-to-gray). Typ panelu IPS z podświetlaniem LED, matowy. Kąty widzenia 178/178 poziom, pion. Złącza HDMI (z HDCP) DisplayPort 15-stykowe D-Sub VG. Beneficjent wymaga dostarczenia kabla HDMI, zgodnego z zaoferowanymi komputerami AiO. Jasność (typ.) Minimum 250 cd/m^2. Kontrast (typ.) 1000:1. Porty USB: Wbudowany hub USB, min. 5x USB3.0. Wymagania funkcjonalne: Możliwość pochylenia panela (tilt). Panel obrotowy (pivot). Regulacja wysokości monitora (height adjustment). Obrotowa podstawa monitora (swivel)

2.1.2.4 TABLET RTK Z ANTENĄ ORAZ DODATKOWĄ TYCZKĄ

Procesor 1,6 GHz, Pamięć RAM 4 GB RAM DDR2, Temperatura pracy -30 °C do +70 °C, Dysk twardy 64 GB, SSD Wyświetlacz panoramiczny 7'' (lub większy) w wysokim kontraście XGA, rozdzielczość 1280x800, czytelny na słońcu ekran dotykowy z regulacją jasności. System operacyjny Microsoft Windows 10 Pro 64 bit PL. Antena Zgodna z Real Time (RTK). Wbudowany odbiornik GPS umożliwiający wyznaczenie współrzędnych geograficznych w czasie rzeczywistym. Dopuszcza się urządzenia z zewnętrznym odbiornikiem GPS RTK zapewniającym bezprzewodowe połączenie (Bluetooth) z tabletem. Wymaga się by dokładność pozioma i pionowa wynosiła: w poziomie: 1 cm + 1 ppm (RMS), w pionie: 1,5 cm + 1 ppm (RMS). Modem 4G LTE zintegrowany w tablecie. Dopuszcza się dostarczenie urządzeń, które będą posiadać ekrany pojemnościowe, z zastrzeżeniem spełniania wymagań dotyczących pracy w pełnym słońcu. Wymaga się by dostarczone urządzenia spełniały normę IP65. Wymaga się, aby dostarczone urządzenia posiadały wytrzymałość na upadki z wysokości minimum 1.2 m, wg MIL-STD-810G. Wymaga się dopuszcza by dostarczone urządzenia posiadały 2 baterie w celu wydłużenia czasu pracy, jednak czas pracy nie może być krótszy niż 14 godzin. Wymaga się, aby oprogramowanie pomiarowe spełniało takie funkcje jak: pomiar, tyczenie, obsługa plików txt, xyz, dxf, dwg, shp. Wymaga się, aby łączna waga zestawu odbiornik z tabletem i kompletem baterii nie wynosiła więcej niż 1800g. Wymaga się wraz z zestawem dostępu do stacji sieci referencyjnych na terenie Polski, których średnia odległość od siebie nie wynosi więcej niż 35 km na okres 1 roku

2.1.2.5 URZADZENIA MONITOROWANIA WARUNKÓW ATMOSFERYCZNYCH

Na potrzeby e-usług publicznych zlokalizowane zostaną urządzenia BRD w postaci stacji meteorologicznych o parametrach dedykowanych dla określonej lokalizacji. Zadaniem stacji meteorologicznych będzie przede wszystkim generowanie informacji na potrzeby zapytań w ramach e-usługi publicznej. Zadaniem stacji meto będzie pomiar wielkości fizycznych opisujących stan nawierzchni drogi i jej otoczenia, przetwarzanie mierzonych wielkości na parametry meteorologiczne, generowanie stanów ostrzegawczych i alarmowych związanych z niebezpiecznymi zjawiskami pogodowymi oraz przekazywanie tych informacji do systemu. Dla potrzeb e-usług urządzenia będą ostrzegały o występowaniu następujących zjawisk pogodowych, stwarzających bezpośrednie zagrożenie dla bezpieczeństwa ruchu drogowego: ostrzeżenie przed oblodzeniem (mokra nawierzchnia spowoduje oblodzenie za 1 – 2 godziny), ostrzeżenie o zmrożeniu (temperatura nawierzchni jest poniżej temperatury zamarzania i temperatura punktu rosy przekracza temperaturę nawierzchni), ostrzeżenie przy występujących opadach przy temperaturze nawierzchni około 0^o C, alarm o gołoledzi na drogach (oblodzenie), ostrzeżenie dla widoczności < 60m, występowanie zjawiska mgły, występowanie intensywnego opadu atmosferycznego, występowanie podmuchów wiatru. jednocześnie dostarczając parametrów pomiarowych

takich jak: temperatura i wilgotność powietrza, intensywność i rodzaj opadu atmosferycznego, widoczność, siła i kierunek wiatru (wartość średnia i maksymalna)
Urządzenia zainstalowane zostaną w wybranych lokalizacjach na maszcie o wysokości 6 m. Stacje meteorologiczne współpracować będą z zespołem czujników pomiarowych, zainstalowanych w nawierzchni jezdni drogi oraz na słupie.

2.1.2.6 KAMERY OBROTOWE

Na potrzeby świadczenia e-usług, zakłada się, iż wykonawca dostarczy urządzenia bezpieczeństwa ruchu drogowego w postaci, kamer monitoringu wizyjnego umożliwiając nadzór drogi we wszystkich warunkach oświetleniowych i pogodowych. Zakłada się wykorzystanie urządzeń, które umożliwiają wykorzystywanie funkcji panoramowania (możliwy obrót dookoła swojej osi o 360° z kontynuacją), zmiany kąta pionowego nachylenia kamery (w taki sposób, aby mieć możliwość obserwacji terenu bezpośrednio pod słupem) i zmiany ogniskowej, aby uzyskać najlepszy możliwy obraz (obiektyw z co najmniej 25 krotnym zoom'em optycznym). Urządzenia będą przekazywały obraz wysokiej jakości HD, zapewniając jakość obrazu w każdych warunkach, pozwalającą na oglądanie wysokiej jakości obrazu. Urządzenia muszą posiadać tryb dzień/noc oraz obudowę co najmniej IP66, identyfikować błędy i zgłaszać je do systemu, reagować na sterowanie przez użytkownika (funkcje panoramowania, zmiany pionowego kąta nachylenia kamery, zmiany ogniskowej) w czasie zbliżonym do rzeczywistego, bez opóźnień.
Do kamer ma zostać zapewniony dostęp w celach konserwacyjnych. Kamery będą posiadały możliwość szybkiego demontażu do przeprowadzenia prac na bezpiecznej wysokości. Jeśli obniżanie kamery będzie się odbywało za pomocą podnośników lub innych urządzeń mechanicznych, zostaną zapewnione środki zapewniające niezawodne działanie systemu. Wymagane parametry kamer obrotowych są następujące: Matryca: 1/2,8" (CMOS); rozdzielczość: 2 MPX (FullHD), Czułość: Color: 0.005 Lux@F1.6; B/W: 0.0005 Lux@F1.6; 0 Lux@F1.6 (IR on), Regulacja ostrości: automatyczna, ręczna, Oświetlacz IR: zasięg 150 m, Zakres regulacji kamery: Pan: 0° ~ 360° endless; Tilt: -15° ~ 90°,auto flip 180°, Zoom optyczny 25x, Kompresja obrazu H.265, Analiza video: przekroczenie wirtualnej linii, przebywanie w obszarze, detekcja poziomu audio. Zasilanie: AC24V/3A(±10%), PoE+(802.3at), Warunki pracy: -40°C ~ 70°C, IP66 Urządzenia winny być fabrycznie nowe, wolne od wad oraz uszkodzeń mechanicznych.

2.1.2.7 KAMERY ANPR

Na potrzeby świadczenia e-usług zakłada się, iż Wykonawca dostarczy urządzenia bezpieczeństwa ruchu drogowego w postaci specjalistycznych stacji monitorowania natężenia ruchu klasy ANPR. Będą one odpowiedzialne za dostarczanie informacji dotyczących ruchu panującego na drogach – w sposób charakterystyczny i określony zasadami działania urządzeń ANPR. Będą działały w oparciu o identyfikację tablic rejestracyjnych. Takie rozwiązanie, w ramach e-usługi, pozwoli na dostarczenie, na wniosek obywateli, danych organom odpowiedzialnym za bezpieczeństwo wewnętrzne. Równocześnie dane te dostępne będą dla wszelkich służb, które zgodnie z prawem mogą wykorzystać te dane na potrzeby prowadzonych przez siebie ustawowych działań tj. Straż Graniczna, Krajowa Administracja Skarbowa, Inspekcja Transportu Drogowego czy GDDKiA. Aby przekazywane w ramach e-usług publicznych, monitorowanie utrudnień w ruchu drogowym było możliwe, platforma zapewni integrację danych napływających z kamery ANPR, kamery obrotowych oraz stacji pogodowych. Platforma zapewni dostęp z jednego miejsca do informacji pochodzących z ww. urządzeń takich jak: obrazy z kamer, informacje o warunkach atmosferycznych pochodzących ze stacji pogodowych (temperatura nawierzchni drogi, powietrza, widoczność, prędkość i kierunek wiatru, intensywność opadów, stan nawierzchni, typ opadów i wilgotność powietrza). Platforma umożliwi automatyczne raportowanie komunikatów ostrzegawczych (alarmów) o niekorzystnych warunkach atmosferycznych i stanach dróg, a warunki wysłania alarmów jak i ich treści będą definiowalne przez użytkownika. Wykonawca winien zastosować w systemie najnowocześniejsze urządzenia ANPR wyposażone w podzespoły najnowszej generacji zapewniające efektywną pracę urządzenia, szybkość przetwarzana danych oraz zapewniające odpowiednią przestrzeń pamięci na

przechowywanie danych wewnątrz urządzenia. Urządzania winny być przystosowane do montażu na konstrukcjach wsporczych. System ANPR winien posiadać minimum następujące funkcjonalności: wykrywanie i automatyczny odczyt tablic rejestracyjnych pojazdów w czasie rzeczywistym, wyszukiwanie odczytanych numerów rejestracyjnych (License Plate Search), ręczne lub półautomatyczne tworzenia listy numerów specjalnego znaczenia (Watch List) – ręczne dodawanie numerów do listy lub import listy z zewnętrznego pliku, dopasowanie numerów (License Plate Match) – automatyczne dopasowanie odczytywanych numerów do numerów z listy i ewentualne wykonanie akcji zdefiniowanej w module reguł, eksport listy do zewnętrznego pliku.
Kamery winny być fabrycznie nowe, wolne od wad oraz uszkodzeń mechanicznych. Wykonawca winien określić parametry techniczne poszczególnych kamer monitoringu, jednakże parametry techniczne kamer nie powinny być gorsze a niżeli: matryca: 1" (CMOS), rozdzielczość: 4096×2160,czułość: 0.03 Lux (F1.6); B&W: 0.0 Lux (IR illuminator) Regulacja ostrości: automatyczna, ręczna Oświetlacz IR: zasięg 150 m (może być zewnętrzny) Kompresja obrazu H.265 Analiza video: Tak (rozpoznawanie typów pojazdów, rozpoznawanie kolorów pojazdów, rozpoznawanie tablic rejestracyjnych, zajętości, średniej długości korka, przekroczenia szybkości) Zasilanie: AC 240V Warunki pracy: -40°C ~ 65°C, IP67. Urządzenia ANPR winny być skonfigurowane z dostarczonymi kamerami IP, dzięki czemu w systemie widoczny będzie nie tylko obraz tablicy rejestracyjnej, ale także obraz całego pojazdu.

System zapewniał będzie archiwizację obrazów statycznych z kamer na serwerze przez okres minimum 12 miesięcy. Oprogramowanie systemów zapewni możliwość automatycznego uzupełniania danych, które nie zostały uprzednio pobrane w wyniku błędów w transmisji. Interfejs użytkownika pozwalał będzie na eksport danych pomiarowych i obrazów, co umożliwi tworzenie dodatkowych archiwów na nośnikach zewnętrznych.
Dane z urządzeń zdalnych wczytywane będą na bieżąco, jak tylko się pojawią (nastąpi moment pobrania obrazu) i archiwizowane na serwerze w formie plików (zdjęcia) lub w bazie danych. Częstotliwość pobierania zależy od zadanego okresu pomiarowego, a wielkość danych pomiarowych wynika z charakterystyki punktu pomiarowego (ilość mierzonych parametrów). W przypadku rozpoznania kończących się zasobów system automatycznie rozpocznie usuwanie zarchiwizowane danych rozpoczynając od najstarszych. Zaproponowana konfiguracja sprzętowa zapewniać będzie minimalnie 12 miesięcy danych archiwalnych dostępnych z poziomu interfejsu użytkownika. Urządzenia winny być fabrycznie nowe, wolne od wad oraz uszkodzeń mechanicznych.

2.1.2.8 ROUTERY Z PRYWATNYM APN

Aby umożliwić świadczenie przez system e-usług, w ramach projektu stworzy się niezawodny, działający w sposób ciągły poprzez utrzymanie komunikacji pomiędzy urządzeniami umieszczonymi w terenie a serwerami systemu.

2.1.2.9 KARTY SIM

Dostarczone zostaną karty SIM w ilościach wskazanych poniżej, poprzez które operator będzie świadczył Beneficjentowi usługę transmisji danych przez okres obowiązywania umowy,
Grupa (ANPR, obrotowe, stacje meteorologiczne) - dostęp do Internetu w technologiach GPRS/EDGE/UMTS/HSDPA, blokowanie połączeń głosowych, możliwa komunikacja P2P (peer-to-peer), miesięczny limit transmisji danych (per SIM), rozliczenie przez pakiety łączone, brak dodatkowych opłat przy przekroczeniu limitów danych, w prywatnym APNie ze statyczną adresacją IP, po wygaśnięciu umowy, karty SIM stają się własnością Beneficjenta.
Access Point Name (APN) - dostarczony powinien charakteryzować się następującymi cechami: APN dla kart SIM musi posiadać łącze współdzielone do Internetu o przepływności przynajmniej 30 Mbps ze statyczną adresacją IP, APN musi zapewnić bezproblemowe i bezpieczne gromadzenie danych z systemu monitorowania dróg, musi zapewnić zdalne zarządzanie urządzeniami sieciowymi z użyciem transmisji pakietowej realizowane przez administratorów systemu, rozliczenie transmisji danych per SIM, brak dodatkowych opłat przy przekroczeniu limitów danych, musi być możliwa komunikacja peer-to-peer pomiędzy kartami SIM, musi mieć możliwość włączenia kart przynajmniej 3 operatorów sieci GSM, dostęp do APN poprzez szyfrowane połączenie VPN.