Znak sprawy:VI.261.17.2020 Załącznik nr 1 do SIWZ

Szczegółowy opis przedmiotu zamówienia
– wymagania minimalne

Nazwa produktu	Opis – wymagane minimalne parametry
1) Komputer- 7 szt.	**Płyta główna:** zaprojektowana na zlecenie producenta jednostki centralnej, z niezamazywaną informacją w BIOS zawierającą nazwę producenta oraz model i nr seryjny/serwisowy komputera. **Procesor:** zgodny z architekturą x64, posiadający co najmniej 6rdzeni fizycznych, osiągający w teście PassMarkPerformanceTestwynik co najmniej 13,340 punktów PassMark CPU Mark High End CPUs (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net w terminie pomiędzy ukazaniem się ogłoszenia a terminem składania ofert). **Karta graficzna:** układ zintegrowany z rdzeniem procesora, osiągający w teście PassMarkPerformanceTest wynik co najmniej 1535 punktów VideocardBenchmarks (wynik zaproponowanego układu graficznego musi znajdować się na stronie https://www.videocardbenchmark.net/ w terminie pomiędzy ukazaniem się ogłoszenia a terminem składania ofert). **Pamięć operacyjna:** min. 16 GB DDR4 o taktowaniu min.2666 MHz pracująca w trybie Dual Channel. **Dysk SSD:** min. 256GB **Dysk twardy:** min. 1TB SATA, 7200 obr./min. **Karta dźwiękowa:** zintegrowana **Karta sieciowa:** zintegrowana typu10/100/1000Mbit/s **Napęd optyczny:** nagrywarka DVD+/-RW DualLayer **Złącza (ilość minimalna):** przedni panel: 2xUSB 2.0, 1xUSB 3.1 Gen.1 (USB 3.0), 1xUSB Type-C; panel tylny: 2xUSB 2.0, 4xUSB 3.1 Gen.1 (USB 3.0), 1xRJ-45 LAN, 2x DisplayPort. Rozmieszczenie interfejsów i ich ilość nie może być osiągnięta na drodze zastosowania kart rozszerzeń przelotek bądź konwerterów. **System operacyjny:** Windows 10 Pro x64 (wersja językowa polska) lub inny spełniający podane w punkcie I (opisane pod

	niniejszą tabelą) warunki równoważności. **Dodatkowe oprogramowanie:** - Oprogramowanie biurowe: MS OFFICE STANDARD 2019 lub inny (licencja bezterminowa, wersja językowa polska) spełniający podane w punkcie II (opisane pod niniejszą tabelą) warunki równoważności. - Oprogramowanie do projektowania graficznego: CorelDRAW Graphics Suite 2020 (licencja wieczysta) lub inne spełniający podane w punkcie III (opisane pod niniejszą tabelą) warunki równoważności. **Dodatkowe wyposażenie:** - klawiatura – sygnowana logo producenta jednostki centralnej - mysz sygnowana logo producenta jednostki centralnej **Typ obudowy komputera:** MT **Kolor:** czarny **Niezawodność / jakość wytwarzania:** Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO9001 oraz ISO 14001. **Gwarancja: min. 12 miesięcy** on-site next business day.
2) Monitor - 7 szt.	**Przekątna ekranu:** min. 23,8” **Rodzaj matrycy:** IPS **Powłoka matrycy:** matowa **Rozdzielczość natywna:** 1920x1080 przy częstotliwości odświeżania 60Hz **Współczynnik proporcji obrazu:** 16:9 **Obsługa kolorów:** 16,7 mln. kolorów **Wielkość plamki:** 0,275 mm **Technologia podświetlenia:** LED **Jasność: min. 250 cd/m2** Złącza (ilość minimalna): 1xVGA, 1xHDMI, 1xDisplayPort,USB 2.0 - 2 szt., USB 3.1 Gen. 1 (USB 3.0) - 2 szt., USB 3.1 Gen. 1 Type-B (USB 3.0) - 1 szt. Obrotowy ekran (PIVOT) - tak **Kolor:** czarny **Dodatkowe wyposażenie:** kabel zasilający, kabel DisplayPort. **Gwarancja: min. 12 miesięcy.**
3) Laptop- 2 szt.	**Procesor:** zgodny z architekturą x64, osiągający w teście PassMarkPerformanceTest wynik co najmniej 5245 punktów PassMark CPU Mark High End CPUs (wynik zaproponowanego procesora musi znajdować sie na stronie http://www.cpubenchmark.net w terminie pomiędzy ukazaniem się ogłoszenia a terminem składania ofert).

	Karta graficzna: zintegrowana. **Dysk twardy:** min. 256GB SSD M.2 PCIe **Pamięć operacyjna:** min. 8 GB DDR4 o taktowaniu min.2666 MHz **Ilość wolnych banków pamięci:** min. 1 szt. **Karta dźwiękowa:** zintegrowana **Karta sieciowa:** zintegrowana typu 10/100 Mbit/s **Bezprzewodowa karta sieciowa:** typu IEEE 802.11a/b/g/n/ac Moduł Bluetooth Urządzenia wskazujące TouchPad Klawiatura numeryczna **Złącza (ilość minimalna):** 1xUSB 2.0, 2xUSB 3.1 Gen.1 (USB 3.0), 1x RJ-45 LAN, 1x HDMI Ilość złączy nie może być osiągnięta na drodze zastosowania przelotek bądź konwerterów. Czytnik kart pamięci Napęd optyczny: : wbudowany lub w formie zewnętrznego urządzenia USB **Wyświetlacz LCD:** Przekątna ekranu: min. 15,6” Typ ekranu: matowy, LED Rozdzielczość natywna: min.1920 x 1080 **Oprogramowanie:** System operacyjny: zainstalowany Windows 10 Pro (wersja językowa polska) lub inny spełniający podane w punkcie I (opisane pod niniejszą tabelą) warunki równoważności. **Dodatkowe oprogramowanie:** Oprogramowanie biurowe: MS OFFICE STANDARD 2019 lub inny (licencja bezterminowa, wersja językowa polska) spełniający podane w punkcie II (opisane pod niniejszą tabelą) warunki równoważności. **Wyposażenie dodatkowe:** - torba dwukomorowa - mysz bezprzewodowa **Niezawodność / jakoś wytwarzania:** Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO9001 oraz ISO 14001. **Gwarancja: min. 12 miesięcy on-site next business day**.
4) **Ekran projekcyjny elektryczny – 1 szt.**	**Powierzchnia projekcyjna:** - kolor biały matowy

wraz z montażem	- przekątna ekranu 85”-90” - proporcje obrazu 16:9 Mocowanie do sufitu lub do ściany Sterowanie**:** pilot bezprzewodowy oraz przełącznik naścienny. **Gwarancja: min. 12 miesięcy.**
5) Projektor + uchwyt sufitowy - 1 szt. wraz z montażem	**Klasa produktu:** projektor multimedialny DLP **Rozdzielczość natywna:** min.1920x1080 **Współczynnik proporcji obrazu:** 16:9 **Współczynnik powiększenia (optyczny):** min. x1,3 **Żywotność lampy:** 3500h - tryb normalny **Jasność (tryb normalny):** min. 3200 ANSI lumen **Kontrast (tryb normalny):** min. 10000:1 Głośniki 10W **Złącza (minimalna ilość):** • 1 x D-sub 15-pin • 2 x HDMI • 1 x RCA audio • 1 x RCA video • 1 x Audio 3.5mm 1 x USB 2.0 • 1 x USBtyp B • 1 x RS-232 **Wyposażenie dodatkowe:** - przewód HDMI – długość min. 15 m. - uchwyt sufitowy długości min. 670 mm, o udźwigu pozwalającym na montaż zaproponowanego projektora. **Gwarancja: min.12 miesięcy** **Wykonanie montażu i konfiguracji urządzeń wskazanych w punktach 4 i 5 niniejszej specyfikacji tj. ekranu projekcyjnego i projektora w lokalizacji: Rzeszów, ul. Dąbrowskiego 33a (Wypożyczalnia Główna)**
6) Komputer - 32 szt.	**Płyta główna:** zaprojektowana na zlecenie producenta jednostki centralnej, z niezamazywaną informacją w BIOS zawierającą nazwę producenta oraz model i nr seryjny/serwisowy komputera. **Procesor:** zgodny z architekturą x64, posiadający co najmniej 4 rdzenie fizyczne, osiągający w teście PassMarkPerformanceTest wynik co najmniej 6,660 punktów PassMark CPU Mark High End CPUs (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net w terminie pomiędzy ukazaniem się ogłoszenia a terminem składania ofert). **Karta graficzna:** układ zintegrowany z rdzeniem procesora,

	osiągający w teście PassMarkPerformanceTest wynik co najmniej 1535 punktów VideocardBenchmarks (wynik zaproponowanego układu graficznego musi znajdować się na stronie https://www.videocardbenchmark.net/ w terminie pomiędzy ukazaniem się ogłoszenia a terminem składania ofert). **Pamięć operacyjna:** min. 8 GB DDR4 o taktowaniu min.2400MHz. **Dysk SSD:** min. 240GB M.2. **Dysk twardy:** min. 1TB SATA. **Karta dźwiękowa:** zintegrowana **Karta sieciowa:** zintegrowana typu 10/100/1000 Mbit/s. **Bezprzewodowa karta sieciowa:** typu IEEE 802.11b/g/n Moduł Bluetooth. **Napęd optyczny:** nagrywarka DVD+/-RW DualLayer **Złącza (ilość minimalna):** przedni panel:2xUSB 3.1 Gen.1 (USB 3.0), czytnik kart pamięci panel tylny: 4xUSB 2.0, 1xRJ-45 LAN, 1xVGA, 1xHDMI. Rozmieszczenie interfejsów i ich ilość nie może być osiągnięta na drodze zastosowania kart rozszerzeń, przelotek bądź konwerterów. System operacyjny: Windows 10 Pro x64 (wersja językowa polska) lub inny spełniający podane w punkcie I (opisane pod niniejszą tabelą) warunki równoważności. **Dodatkowe oprogramowanie:** - Oprogramowanie biurowe: MS OFFICE STANDARD 2019 lub inny (licencja bezterminowa, wersja językowa polska) spełniający podane w punkcie II (opisane pod niniejszą tabelą) warunki równoważności. **Dodatkowe wyposażenie:** -klawiatura – sygnowana logo producenta jednostki centralnej - mysz sygnowana logo producenta jednostki centralnej **Typ obudowy komputera:** SFF **Kolor:** czarny **Niezawodność / jakość wytwarzania:** Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO9001 oraz ISO 14001. **Gwarancja: min. 12miesięcy** on-site next business day.
7) Monitor - 32 szt.	**Przekątna ekranu:** min. 21,5”

	Rodzaj matrycy: IPS **Powłoka matrycy:** matowa **Rozdzielczość natywna:** min. 1920x1080 przy częstotliwości odświeżania 60Hz **Kontrast statyczny:** min. 1000:1 **Jasność:** min. 250:1 **Współczynnik proporcji obrazu:** 16:9 **Obsługa kolorów:** min. 16,7 mln. kolorów **Wielkość plamki:** max. 0,248 mm **Technologia podświetlenia:** LED **Złącza (ilość minimalna):** 1xVGA, 1xHDMI, **Kolor:** czarny **Dodatkowe wyposażenie:** kabel zasilający, kabel HDMI. **Gwarancja: min. 12 miesięcy.**
8) Urządzenie do regeneracji płyt CD, DVD, Blu-ray- 1 szt. + dodatkowy zestaw naprawczy	Wykorzystana technologia polerująca: Advanced Hydro Optic Pełna automatyzacja procesu regeneracji płyt Elektroniczny chip do kontroli zużycia materiałów eksploatacyjnych. Tryb pracy: jednokrokowy Wydajność: regeneracja min. 300 płyt dziennie Wzmocniona stalowa obudowa Zestaw naprawczy: na min.500 procesów jednominutowych. **Gwarancja: min. 12 miesięcy.**
9) Taśmy magnetyczne LTO – 8 szt.	Typ nośnika: LTO-4 Pojemność natywna: 800 GB Pojemność z kompresją: 1600 GB **Gwarancja: min. 12 miesięcy.**
10) Urządzenie wielofunkcyjne – 7 szt.	Podstawowe funkcje urządzenia: kopiarka, drukarka, skaner Technologia druku – laserowa Maksymalny rozmiar papieru – min. A4 Rozdzielczość druku : min. – 600x 600 dpi Szybkość wydruku – min. 38 str/min Łączność: Port USB 2.0, Lan, WiFi Automatyczny duplex Automatyczne kopiowanie dwustronne Automatyczny podajnik dokumentów Wyświetlacz – kolorowy, wbudowany Drukowanie ze smartfonów i tabletów Skaner Optyczna rozdzielczość skanowania: min.600 x 600 dpi Format plików: PDF, JPG Skanowanie do e-maila.

	Gwarancja min. 12 miesięcy.
11) Urządzenie wielofunkcyjne atramentowe – 5 szt.	Podstawowe funkcje urządzenia: kopiarka, drukarka, skaner Technologia druku: Atramentowa, kolorowa Rozdzielczość maksymalna: min 6000x1200 dpi Maksymalny rozmiar papieru – min. A4 Szybkość druku w kolorze – min. 10 str./min Szybkość druku w mono – min. 27 str./min Rozdzielczość skanowania optyczna: min.1200x2400dpi Obsługiwany typ nośnika: Papier zwykły, papier fotograficzny, koperty, etykiety Interfejsy: USB, Wi-Fi Wyświetlacz – wbudowany Drukowanie ze smartfonów i tabletów **Gwarancja min. 12 miesięcy.**
12) Czytnik e-booków + twarde etui - 29 szt.	Ekran: min. 6 cali w technologii e-papieru E-InkCarta Rozdzielczość: min. 1024x758 , interfejs dotykowy, 16 poziomów szarości. Obsługiwane formaty plików: PDF, EPUB, DJVU, FB2, FB2.ZIP, DOC, DOCX, RTF, PRC, TCR, TXT, CHM, HTM, HTML, MOBI, ACSM, JPEG, BMP, PNG, TIFF Bateria: min. 1500 mAh Pamięć RAM: min. 512 MB Pamięć wewnętrzna: min.8 GB Obsługa sieci bezprzewodowych: Wi-Fi (802.11b/g/n) Porty (minimalna ilość): micro-USB, port karty pamięci microSD do 32 GB Funkcje dodatkowe: Legimi, przeglądarka internetowa Wyposażenie dodatkowe: **twarde etui**. Etui posiada funkcję automatycznego usypiania i wybudzania czytnika. Zamykane na magnes. **Gwarancja min. 12 miesięcy.**
13) Zakup systemu monitorowania i tworzenia backupu dla zasobów serwerów oraz optymalizacji danych (VEEAM)	Zamawiający wymaga dostarczenia środowiska wykonywania kopii zapasowych i monitorowania dla co najmniej 50 VM pracujących w środowisku VMware (5 serwerów fizycznych, 2 procesorowych) oraz 5 użytkowników aplikacji Office 365 spełniającego łącznie wszystkie poniższe wymagania funkcjonalne: • Oprogramowanie musi być dostarczone z co najmniej 12-miesięcznym wsparciem technicznym producenta

	zapewniającym dostęp do poprawek, najnowszych wersji oprogramowania oraz pomocy technicznej producenta. • 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, 7.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMwarevCenter oraz pojedynczymi hostami. • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. • Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków. • Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental). • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w

	tej specyfikacji. • Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. • Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft AzureBlob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania. • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. • Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time). • Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu. • Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API. • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji. • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji. • Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.

	• Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX). • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. • Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej. • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego, tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych. • Oprogramowanie musi oferować ten mechanizm z dokładnością do datastoru. • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphanedsnapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage. • Oprogramowanie musi posiadać wsparcie dla VMwarevSAN potwierdzone odpowiednią certyfikacją VMware. • Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn. • Oprogramowanie musi posiadać wsparcie dla NDMP. • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son). • Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.

	• Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym CatalystCopy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. • Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. • Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMwarevSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik. • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replicaseeding). • Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V. • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN). • Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere. • Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallelprocessing). • Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. • Dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). • Oprogramowanie musi pozwalać na migrację on-line

	tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami. • Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre. • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft AzureStack oraz Amazon EC2. • Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików. • Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. • Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: o **Linux** ▪ ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs o **BSD** ▪ UFS, UFS2 o **Solaris** ▪ ZFS, UFS o **Mac** ▪ HFS, HFS+ o **Windows** ▪ NTFS, FAT, FAT32, ReFS o **Novell OES** ▪ NSS • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. • Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z

	AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "PermanentlyDeleted Objects"), • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień. • Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. • Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego. • Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN. • Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN. • Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem. • Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere. • Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania

	skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. • Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. • System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMwarevSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich. • System musi umożliwiać monitorowanie środowiska wirtualizacyjnegoVMware w wersji 5.x oraz 6.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie. • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. • System musi mieć status „VMwareReady" i być przetestowany i certyfikowany przez Vmware. • System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter. • System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn. • System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel. • System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk. • System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora. • System musi mieć wbudowane połączenie z bazą

	wiedzy opisującą problemy z predefiniowanych alarmów. • System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard). • System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna. • System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego. • System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta. • System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. • System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. • System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware. • System musi mieć możliwość monitorowania instancji VMwarevCloudDirector w wersji 8.x i 9.x. • System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.x oraz 6.x vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019. • System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. • System musi być certyfikowany przez VMware i

	posiadać status „VMwareReady”. • System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V. • System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF. • System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc. • System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach. • System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów. • System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych. • System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych. • System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury. • System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta. • System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. • System musi mieć możliwość generowania raportu planowania pojemności (capacityplanning) bazującego na scenariuszach ‘what-if’. • System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.

	• System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphanedsnapshots). • System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie. • Rozwiązanie musi wykonywać kopię zapasową danych Microsoft Exchange Online w ramach usługi Office365 oraz lokalnych instancji Microsoft Exchange. • Rozwiązanie musi wykonywać kopię zapasową danych Microsoft Sharepoint Online w ramach usługi Office365 oraz lokalnych instancji Microsoft Sharepoint. • Rozwiązanie musi wykonywać kopię zapasową danych Microsoft OneDrive for Business w ramach usługi Office365. • Rozwiązanie musi pozwalać na dodanie wielu subskrypcji Office365 oraz wielu lokalnych serwerów Exchange oraz Sharepoint. • Rozwiązanie nie może instalować żadnych agentów po stronie lokalnych instancji Exchange oraz Sharepoint. Wymaga się wykorzystania API wewnętrznych aplikacji. • Rozwiązanie nie może wymagać tworzenia dodatkowych elementów/agentów po stronie Office365. • Rozwiązanie musi wspierać uwierzytelnianie wieloskładnikowe (MFA). • Rozwiązanie musi posiadać skalowalną architekturę (serwer zarządzający, repozytorium). Nie dopuszcza się, aby komponenty systemu backupu były dodatkowo licencjonowane. • Rozwiązanie musi przechowywać dane w macierzystym formacie Microsoft Exchange. • Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft Exchange (skrzynka, mail, kontakt, wpis z kalendarza, element folderu „PermanentlyDeletedItems”). • Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft Sharepoint. Opcja odtworzenia elementów, witryn. • Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft OneDrive. Opcja odtworzenia plików, folderów lub całych kont OneDrive. • Rozwiązanie musi pozwalać na odzysk elementów do skrzynki w pakiecie Office 365, lokalnej skrzynki Exchange, pliku oraz w formacie PST. • Rozwiązanie musi pozwalać na hybrydowe scenariusze

	backupu/odzysku (np. backup wykonany z lokalnej instancji Exchange, odzysk do Exchange Online w Office365). • Rozwiązanie musi pozwalać na granularne przeszukiwanie zabezpieczonych danych (eDiscovery). • Rozwiązanie musi mieć możliwość integracji z innymi rozwiązanymi poprzez PowerShell oraz RESTful API. • Rozwiązanie musi posiadać integrację z posiadanym centralnym systemem backupu.
14) Wielofunkcyjna zapora sieciowa – 3 szt.	**Wymagania ogólne** 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 3 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** 1. 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. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną

	oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. **Interfejsy, dysk, zasilanie:** 1. System realizujący funkcję Firewall musi dysponować minimum: • 5 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilacz. **Parametry wydajnościowe:** 1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps. **Funkcje Systemu Bezpieczeństwa:** W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy StatefulInspection. 2. Kontrola Aplikacji.

	3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - IntrusionPrevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Trafficshaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. **Polityki, Firewall** 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMwarevCenter (ESXi).

	Połączenia VPN 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. **Routing i obsługa łączy WAN** 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o

	protokoły: RIPv2, OSPF, BGP oraz PIM. **Zarządzanie pasmem** 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. **Ochrona przed malware** 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. **Ochrona przed atakami** 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

	5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. **Kontrola aplikacji** 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. **Kontrola WWW** 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja SafeSearch – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

	6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. **Uwierzytelnianie użytkowników w ramach sesji** 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. **Zarządzanie** 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne,

	przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. **Logowanie** 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. **Certyfikaty** Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA dla funkcji Firewall. **Serwisy i licencje** W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy. **Gwarancja oraz wsparcie** Gwarancja: System musi być objęty serwisem gwarancyjnym

	przez **okres 12 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.

Wszystkie pozycje, w których wymieniono nazwy firmowe sprzętu, oprogramowania lub pozostałego wyposażenia, można zastąpić analogicznymi (równoważnymi) pozycjami innego producenta, jednak o parametrach technicznych i użytkowych nie gorszych od określonych w niniejszym opisie przedmiotu zamówienia.

Warunki równoważności:

I. System operacyjny 64-bit. Za rozwiązanie równoważne uznaje się takie, które posiada wbudowane mechanizmy, bez użycia dodatkowych aplikacji (bez jakichkolwiek emulatorów, implementacji lub programów towarzyszących), zapewniające:

1. polską wersję językową,

2. możliwość instalacji i poprawnego działania oprogramowania dostępnego w ramach posiadanych przez Zamawiającego licencji Microsoft Office 2016,

3. możliwość instalacji i poprawnego działania aplikacji wykorzystywanych przez Zamawiającego, oraz poprawnej obsługi powszechnie używanych urządzeń peryferyjnych (drukarek, skanerów, kser),

4. dostępność aktualizacji i poprawek do systemu u producenta systemu bezpłatnie i bez dodatkowych opłat licencyjnych,

5. graficzne środowisko instalacji i konfiguracji,

6. możliwość udostępniania plików i drukarek,

7. zapewnienie wsparcia dla większości powszechnie używanych urządzeń (drukarek, urządzeń sieciowych, standardów USB, urządzeń Plug & Play, WiFi),

8. wyposażenie systemu w graficzny interfejs użytkownika w języku polskim,

9. zapewnienie pełnej kompatybilności zaoferowanym sprzętem,

10. zintegrowanie z systemem modułu pomocy dla użytkownika w języku polskim,

11. zintegrowanie z systemem modułu wyszukiwania informacji,

12. zabezpieczony hasłem hierarchiczny dostęp do systemu, praca systemu w trybie ochrony kont użytkowników,

13. zintegrowane z systemem operacyjnym, narzędzia zwalczające złośliwe oprogramowanie, aktualizacja dostępna u producenta nieodpłatnie bez ograniczeń czasowych,

14. licencja na system operacyjny musi być nieograniczona w czasie, pozwalać na wielokrotne instalowanie systemu na oferowanym sprzęcie bez konieczności kontaktowania się przez Zamawiającego z producentem systemu lub sprzętu,

15. oprogramowanie musi umożliwiać prace w domenie,

16. oprogramowanie powinno posiadać certyfikat autentyczności lub unikalny kod aktywacyjny,

17. zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie systemów.

II. Zamawiający uzna pakiet oprogramowania biurowego za równoważny określonemu w SIWZ, gdy spełni poniższe wymagania:

Oprogramowanie biurowe w najnowszej dostępnej na rynku wersji. Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.

Dla oprogramowania musi być publicznie znany cykl życia, przedstawiony przez producenta systemu i dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa.

Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie przez producenta na jego stronie internetowej w okresie co najmniej 5 lat.

Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta.

Zawierające w pakiecie przynajmniej edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji.

Aplikacja do tworzenia prezentacji powinna umożliwiać udostępnianie prezentacji przy użyciu przeglądarki internetowej bez potrzeby instalowania dodatkowych elementów ani konfigurowania.

Pliki programów edytora tekstów, arkusza kalkulacyjnego i programu do tworzenia prezentacji można przechowywać online i uzyskiwać do nich dostęp, przeglądać, edytować i udostępniać inny użytkownikom.

Pakiet biurowy musi spełniać następujące wymagania:

1. Wymagania odnośnie interfejsu użytkownika:

a. Pełna polska wersja językowa interfejsu użytkownika.

b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:

a. Posiada kompletny i publicznie dostępny opis formatu.

b. Umożliwia wykorzystanie schematów XML.

3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.

4. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).

5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.

6. Pakiet zintegrowanych aplikacji biurowych musi zawierać:

a. Edytor tekstów.

b. Arkusz kalkulacyjny.

c. Narzędzie do przygotowywania i prowadzenia prezentacji.

d. Narzędzie do tworzenia drukowanych materiałów informacyjnych.

e. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

7. Edytor tekstów musi umożliwiać:

a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.

b. Wstawianie oraz formatowanie tabel.

c. Wstawianie oraz formatowanie obiektów graficznych.

d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).

e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.

f. Automatyczne tworzenie spisów treści.

g. Formatowanie nagłówków i stopek stron.

h. Sprawdzanie pisowni w języku polskim.

i. Śledzenie zmian wprowadzonych przez użytkowników.

j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.

k. Określenie układu strony (pionowa/pozioma).

l. Wydruk dokumentów.

m. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.

n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.

p. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających odpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

8. Arkusz kalkulacyjny musi umożliwiać:

a. Tworzenie raportów tabelarycznych.

b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.

c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.

d. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.

e. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.

f. Wyszukiwanie i zamianę danych.

g. Wykonywanie analiz danych przy użyciu formatowania warunkowego.

h. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.

i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.

j. Formatowanie czasu, daty i wartości finansowych z polskim formatem.

k. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.

l. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, 2013, 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.

m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

a. Przygotowywanie prezentacji multimedialnych, które będą:

b. Prezentowanie przy użyciu projektora multimedialnego.

c. Drukowanie w formacie umożliwiającym robienie notatek.

d. Zapisanie jako prezentacja tylko do odczytu.

e. Nagrywanie narracji i dołączanie jej do prezentacji.

f. Opatrywanie slajdów notatkami dla prezentera.

g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.

h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.

i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.

j. Możliwość tworzenia animacji obiektów i całych slajdów.

k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.

l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010, 2016.

10. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:

a. Tworzenie i edycję drukowanych materiałów informacyjnych.

b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.

c. Edycję poszczególnych stron materiałów.

d. Podział treści na kolumny.

e. Umieszczanie elementów graficznych.

f. Wykorzystanie mechanizmu korespondencji seryjnej.

g. Płynne przesuwanie elementów po całej stronie publikacji.

h. Eksport publikacji do formatu PDF oraz TIFF.

i. Wydruk publikacji.

j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.

11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.

b. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.

c. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.

d. Automatyczne grupowanie poczty o tym samym tytule.

e. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.

f. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia.

g. Zarządzanie kalendarzem.

h. Udostępnianie kalendarza innym użytkownikom.

i. Przeglądanie kalendarza innych użytkowników.

j. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.

k. Zarządzanie listą zadań.

l. Zlecanie zadań innym użytkownikom.

m. Zarządzanie listą kontaktów.

n. Udostępnianie listy kontaktów innym użytkownikom.

o. Przeglądanie listy kontaktów innych użytkowników.

p. Możliwość przesyłania kontaktów innym użytkownikom.

III. Zamawiający uzna oprogramowanie do projektowania graficznego za równoważne określonemu w SIWZ, gdy spełni poniższe wymagania:

Oprogramowanie graficzne w najnowszej dostępnej na rynku wersji. Zamawiający nie dopuszcza zaoferowania programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.

Zamawiający wymaga, aby wszystkie elementy oprogramowania graficznego oraz jego licencja pochodziły od tego samego producenta.

Oprogramowanie musi umożliwiać

1. tworzenie grafiki wektorowej,
2. edycję grafiki rastrowej, przy użyciu warstw,
3. zarządzanie czcionkami,
4. przekształcanie map bitowych w edytowalne grafiki wektorowe,
5. edycja obrazów w formacie RAW.

Zamawiający:
mgr Barbara Chmura
p.o. Dyrektor WiMBP w Rzeszowie