Nr postępowania: **RGKiM.271.3.2023.ACH** ***Załącznik nr 6 do SWZ***

ZMIANA Z DNIA 23.03.2023

Opis Przedmiotu Zamówienia (OPZ)

Dla zadania pn.

Zakup i dostawa sprzętu teleinformatycznego dla Gminy Miasta Puck

w podziale na 3 części:

Część 1:

I. Zakup i dostawa sprzętu komputerowego dla jednostek podległych Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina"

II. Ogólny opis przedsięwzięcia

1. Przedmiotem niniejszego zamówienia jest:
   - Zakup i dostawa 20 komputerów przenośnych dla Szkoły Podstawowej w Pucku. Dostawa: Szkoła Podstawowa im. Mariusza Zaruskiego w Pucku, ul. Przebendowskiego 27, 84-100 Puck
   - Zakup i dostawa 4 zestawów komputerów stacjonarnych i 1 komputera przenośnego (z zainstalowanym systemem operacyjnym Windows 11 PRO – licencja nie EDU) dla Miejskiej Biblioteki Publicznej w Pucku wraz z oprogramowaniem biurowym.
     Dostawa: Biblioteka Publiczna im. Zaślubin Polski z Morzem w Pucku 84-100 Puck, Sambora 16
2. Dostawa odbywa się w formie jednorazowej.

Opis komputera przenośnego szt. 21

Nazwa	Wymagane minimalne parametry techniczne
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej,
Matryca	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości FHD (1920 x 1080) z podświetleniem WLED matryca matowa, jasność min. 235nits,
Wydajność	Notebook w oferowanej konfiguracji musi osiągać w teście Bapco Mobile Mark25 wyniki nie gorsze niż: Productivity – minimum 730 punktów DC Performance – minimum 700 pkt MobileMark 25 indeks – minimum 275 pkt Wymagane testy wydajnościowe wykonawca musi przeprowadzić na

	automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.) Potwierdzeniem spełnienia powyższych wymagań będzie dołączony do oferty wydruk raportu z oprogramowania testującego. Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych testów Wykonawca może zostać wezwany przy dostawie do wykonania w obecności Zamawiającego, na dwóch losowo wskazanych przez Zamawiającego notebookach, testów ich wydajności, zgodnie z powyższymi wymaganiami, potwierdzający zadeklarowane przez Wykonawcę wyniki wydajnościowe
Pamięć RAM	8GB DDR4 możliwość rozbudowy do min 16GB, dwa sloty pamięci (nie dopuszcza się pamięci wlutowanych); możliwość rozbudowy pamięci przez użytkownika, bez kontaktu z serwisem producenta.
Pamięć masowa	min. 256 GB SSD NVMe,
Karta graficzna	Zintegrowana z procesorem
Multimedia	Dwukanałowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki stereo, cyfrowy mikrofon z funkcją macierzy podwójnej Kamera internetowa o rozdzielczości min. HD trwale zainstalowana w obudowie matrycy,
Bateria i zasilanie	Zasilacz o mocy min. 45W. Konstrukcja komputera musi umożliwiać demontaż samej baterii lub wszystkich zainstalowanych baterii w okresie gwarancyjnym. Bateria nie może być trwale zespolona z płytą główną.
Waga	Waga komputera z oferowaną baterią nie większa niż 1,75 kg
Certyfikaty	Oferowane laptopy muszą posiadać europejską deklarację zgodności CE, Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.
System operacyjny	Zainstalowany system operacyjny Windows 11 Professional z możliwością downgrade'u do Win 10 Pro lub równoważny zgodnie z Kryteriami równoważności znajdującymi się w załączniku nr 1 do Opisu Przedmiotu Zamówienia*. Nie dopuszcza się w tym zakresie licencji pochodzących z rynku wtórnego umieszczony na obudowie Certyfikat Autentyczności w postaci specjalnej naklejki zabezpieczającej lub Załączone potwierdzenie wykonawcy / producenta komputera o legalności dostarczonego oprogramowania systemowego.
Wymagania dodatkowe	Wbudowane porty i złącza: HDMI 1.4, RJ-45 (karta sieciowa wbudowana), min. 2xUSB w tym min. 2 port USB 3.2 gen1 typ-A, czytnik kart SD, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, złącze zasilania (zasilacz nie może zajmować portów USB) Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11AC, moduł bluetooth 5.0

	Klawiatura (układ US - QWERTY) z wydzieloną klawiaturą numeryczną, Wielodotykowy touchpad, funkcja gestów, precyzyjny panel dotykowy, gładzik z certyfikatem PTP.
Warunki gwarancji	3-letnia gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego. Dostawca musi posiadać: Dedykowany portal chmurowy do zgłaszania awarii lub usterek zabezpieczony protokołem SSL Możliwość logowania się do systemu z przeglądarki Firefox, Chrome, safari, opera, edge, internet Explorer Logowanie do systemu za pomocą loginu: własnego adresu e-mail i hasła, które użytkownik może samodzielnie zmienić System musi mieć możliwość dodania minimum 100 urządzeń System musi mieć możliwość przypisania do urządzenia - numeru seryjnego sprzętu - minimum 2 numerów wewnętrznych potrzebnych do wewnętrznej identyfikacji oraz inwentaryzacji sprzętu System musi posiadać możliwość generowania kodów QR dla danego produktu uwzględniając jego numer seryjny do zgłaszania usterek poprzez SMS lub Strefę Klienta W panelu klienta użytkownik musi mieć możliwość zobaczyć wykaz urządzeń wraz z numerem seryjnym oraz numerami wewnętrznymi W panelu klienta użytkownik musi mieć możliwość zgłoszenia usterki urządzenia wybierając konkretne urządzenie W panelu klienta musza znajdować się wszystkie zgłoszenia oraz musi być możliwość ich filtracji po numerze seryjnym, modelu lub marce urządzenia

Opis komputera stacjonarnego szt. 4

Nazwa komponentu	Wymagane parametry techniczne komputerów
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych. Procesor minimum 4 rdzeniowy osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 13800 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php.
Pamięć RAM	8GB DDR4 3200MHz. Możliwość rozbudowy do min 64GB.
Pamięć masowa	Dysk M.2 SSD 256GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”.
Wydajność grafiki	Zintegrowana karta graficzna
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo.
Obudowa	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Obudowa fabrycznie

	przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 mm. Zasilacz o mocy min. 150W pracujący w sieci 230V 50/60Hz prądu Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów

	SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
System operacyjny	Zainstalowany system operacyjny Windows 11 Professional, musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu lub równoważny, co najmniej w zakresie projektowania, produkcji i serwisu komputerów. Oferowane komputery stacjonarne muszą posiadać europejską deklarację zgodności CE. Producent komputera/fabryka producenta musi spełniać normę ISO 50001 lub równoważną. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram.
Wymagania dodatkowe	Wbudowane porty: 1 x HDMI 1.4 1 x DisplayPort 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: Panel przedni: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 Panel tylny: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu 1 x RJ – 45 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub

	przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0. Jedno złącze M.2 dla dysków. Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Warunki gwarancji	Dostawca musi posiadać: Dedykowany portal chmurowy do zgłaszania awarii lub usterek zabezpieczony protokołem SSL Możliwość logowania się do systemu z przeglądarki Firefox, Chrome, safari, opera, edge, internet Explorer Logowanie do systemu za pomocą loginu: własnego adresu e-mail i hasła, które użytkownik może samodzielnie zmienić System musi mieć możliwość dodania minimum 100 urządzeń System musi mieć możliwość przypisania do urządzenia - numeru seryjnego sprzętu - minimum 2 numerów wewnętrznych potrzebnych do wewnętrznej identyfikacji oraz inwentaryzacji sprzętu System musi posiadać możliwość generowania kodów QR dla danego produktu uwzględniając jego numer seryjny do zgłaszania usterek poprzez SMS lub Strefę Klienta W panelu klienta użytkownik musi mieć możliwość zobaczyć wykaz urządzeń wraz z numerem seryjnym oraz numerami wewnętrznymi W panelu klienta użytkownik musi mieć możliwość zgłoszenia usterki urządzenia wybierając konkretne urządzenie W panelu klienta musza znajdować się wszystkie zgłoszenia oraz musi być możliwość ich filtracji po numerze seryjnym, modelu lub marce urządzenia

Opis monitora szt. 4

Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą IPS 23,8”
Rozmiar plamki (maksymalnie)	0,275mm x 0,275mm
Jasność	250 cd/m2
Kontrast	Min. 1000:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy	Max 8ms (gray to gray)

Rozdzielczość maksymalna	1920 x 1080
Powłoka powierzchni ekranu	Antyodblaskowa
Podświetlenie	System podświetlenia LED
Zużycie energii	Maksymalnie 28W
Bezpieczeństwo	Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą
Złącza	1x VGA, 1x HDMI,
Gwarancja	3-letnia gwarancja producenta świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego
Certyfikaty	EPEAT Gold (2018) dla Polski lub równoważny Monitor musi się znajdować na stronie TCO : http://tcocertified.com/product-finder/
Inne	VESA 100mm
Nazwa komponentu	Wymagane minimalne parametry techniczne monitora

Opis oprogramowania - pakiet biurowy szt. 5

Oprogramowanie biurowe (5 sztuk)	Oprogramowanie biurowe typu Microsoft Office 2019 z licencją bezterminową lub równoważne***** **zgodnie z Kryteriami równoważności** znajdującymi się w załączniku nr 1 do Opisu Przedmiotu Zamówienia. Zamawiający wymaga oprogramowania, nieużywanego oraz nieaktywowanego nigdy wcześniej na urządzeniach.
Okres licencji	Wieczysta
Rodzaj licencji	PKC
Wersja językowa	Polska

III. Pozostałe elementy zamówienia

3. Ponadto Wykonawca w cenie oferty zobowiązuje się ująć koszty m.in.:

Wykonania i umieszczenia naklejek na potrzeby oznakowania każdego urządzenia zgodnie z zasadami promocji i oznakowania projektów w Programie Polska Cyfrowa w szczególności zgodnie z Kartą wizualizacji Programu Polska Cyfrowa na lata 2014-2020 - wg. załącznika nr 2 do OPZ

4. Forma wynagrodzenia ryczałtowego (art. 632 KC) wymaga od Wykonawcy również wyceny ryzyka, bowiem Wykonawca nie będzie mógł żądać zmiany wynagrodzenia ryczałtowego dla zakresu dostaw objętych niniejszym zamówieniem.

5. Wykonawca jest odpowiedzialny za staranne zaznajomienie się z dokumentacją przetargową.

6. Wykonawca przed zawarciem umowy **przedłoży Zamawiającemu kosztorys ofertowy w formie uproszczonej.**
7. RODO: Dane osobowe Wykonawcy dostaw, podwykonawców oraz dane zawarte w dokumentacji powykonawczej będą przechowywane przez cały okres trwania gwarancji.

Część 2:

IV. Zakup, dostawa i instalacja sprzętu teleinformatycznego dla jednostek podległych Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina"

V. Ogólny opis przedsięwzięcia

1. Przedmiotem niniejszego zamówienia jest zakup, dostawa, konfiguracja (opisana pkt. 3) i instalacja sprzętu teleinformatycznego typu zapora sieciowa dla jednostek podległych Gminy Miasta Puck:

- Miejski Ośrodek Pomocy Społecznej w Pucku (MOPS)- szt. 1
- Biblioteka Publiczna im. Zaślubin Polski z Morzem w Pucku (Biblioteka) - szt. 1
- Szkoła Podstawowa im. Mariusza Zaruskiego w Pucku (SP) - szt. 2

2. Dostawa i instalacje zgodnie z harmonogramem ustalonym z Zamawiającym.

Dostawa:

MOPS ul. 1 Maja 13, 84-100 Puck

Biblioteka 84-100 Puck, Sambora 16

SP ul. Przebendowskiego 27, 84-100 Puck

3. Konfiguracja:

- uruchomienie urządzenie
- aktualizacja firmware
- konfiguracja portów WAN i LAN
- konfiguracja polityk bezpieczeństwa wspieranych przez dostarczoną zaporę sieciową

Parametry techniczne zapory sieciowej typ 1 (MOPS, Biblioteka)

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę 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 wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 5 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

1. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

1. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 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 protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. 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 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
1. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
1. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
1. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
1. Element systemu realizujący funkcję Firewall integruje 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.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - 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.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.

- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia 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).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia 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.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

1. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

1. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres **24** miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24 x7.

2. Dostawca musi posiadać:
   Dedykowany portal chmurowy do zgłaszania awarii lub usterek zabezpieczony protokołem SSL
   Możliwość logowania się do systemu z przeglądarki Firefox, Chrome, safari, opera, edge, internet Explorer
   Logowanie do systemu za pomocą loginu: własnego adresu e-mail i hasła, które użytkownik może samodzielnie zmienić
   System musi mieć możliwość dodania minimum 100 urządzeń

System musi mieć możliwość przypisania do urządzenia
- numeru seryjnego sprzętu
- minimum 2 numerów wewnętrznych potrzebnych do wewnętrznej identyfikacji oraz inwentaryzacji sprzętu

System musi posiadać możliwość generowania kodów QR dla danego produktu uwzględniając jego numer seryjny do zgłaszania usterek poprzez SMS lub Strefę Klienta

W panelu klienta użytkownik musi mieć możliwość zobaczyć wykaz urządzeń wraz z numerem seryjnym oraz numerami wewnętrznymi

W panelu klienta użytkownik musi mieć możliwość zgłoszenia usterki urządzenia wybierając konkretne urządzenie

W panelu klienta musza znajdować się wszystkie zgłoszenia oraz musi być możliwość ich filtracji po numerze seryjnym, modelu lub marce urządzenia

Parametry techniczne zapory sieciowej typ 2 (Szkoła Podstawowa)

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę 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 wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

1. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

1. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. 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 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

1. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.

1. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

1. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

1. Element systemu realizujący funkcję Firewall integruje 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.
   - VMware NSX.

- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - 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.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia 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).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia 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.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

1. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

1. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje(dołączyć do oferty):

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2. Dostawca musi posiadać:
   Dedykowany portal chmurowy do zgłaszania awarii lub usterek zabezpieczony protokołem SSL
   Możliwość logowania się do systemu z przeglądarki Firefox, Chrome, safari, opera, edge, internet Explorer
   Logowanie do systemu za pomocą loginu: własnego adresu e-mail i hasła, które użytkownik może samodzielnie zmienić
   System musi mieć możliwość dodania minimum 100 urządzeń
   System musi mieć możliwość przypisania do urządzenia
   - numeru seryjnego sprzętu
   - minimum 2 numerów wewnętrznych potrzebnych do wewnętrznej identyfikacji oraz inwentaryzacji sprzętu
   System musi posiadać możliwość generowania kodów QR dla danego produktu uwzględniając jego numer seryjny do zgłaszania usterek poprzez SMS lub Strefę Klienta
   W panelu klienta użytkownik musi mieć możliwość zobaczyć wykaz urządzeń wraz z numerem seryjnym oraz numerami wewnętrznymi
   W panelu klienta użytkownik musi mieć możliwość zgłoszenia usterki urządzenia wybierając konkretne urządzenie
   W panelu klienta musza znajdować się wszystkie zgłoszenia oraz musi być możliwość ich filtracji po numerze seryjnym, modelu lub marce urządzenia

VI.

VII. <u>Pozostałe elementy zamówienia</u>

4. Ponadto Wykonawca w cenie oferty zobowiązuje się ująć koszty m.in.:

   1) Wykonania i umieszczenia naklejek na potrzeby oznakowania każdego urządzenia zgodnie z zasadami promocji i oznakowania projektów w Programie Polska Cyfrowa w szczególności zgodnie z Kartą wizualizacji Programu Polska Cyfrowa na lata 2014-2020 - wg. załącznika nr 2 do OPZ.

5. Forma wynagrodzenia ryczałtowego (art. 632 KC) wymaga od Wykonawcy również wyceny ryzyka, bowiem Wykonawca nie będzie mógł żądać zmiany wynagrodzenia ryczałtowego dla zakresu dostaw objętych niniejszym zamówieniem.

6. Wykonawca jest odpowiedzialny za staranne zaznajomienie się z dokumentacją przetargową.

7. **<u>Wykonawca przed zawarciem umowy przedłoży Zamawiającemu kosztorys ofertowy w formie uproszczonej.</u>**

8. RODO: Dane osobowe Wykonawcy dostaw, podwykonawców oraz dane zawarte w dokumentacji powykonawczej będą przechowywane przez cały okres trwania gwarancji.

Część 3:

Zakup, dostawa i instalacja systemu Backup z oprogramowaniem dla Urzędu Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina"

VIII. Ogólny opis przedsięwzięcia

8. Przedmiotem niniejszego zamówienia jest zakup, dostawa i instalacja systemu Backup z oprogramowaniem dla Urzędu Miasta Puck
Dostawa Urząd Miasta Puck, ul. 1 Maja 13, 84-100 Puck

9. Dostawa i instalacja odbywa się w formie jednorazowej.

1. Przedmiotem niniejszego postepowania jest
   - 1.1. Dostawa dwóch serwerów typu Rack wraz z wykonaniem montażu w serwerowni Zamawiającego zgodnie z załącznikiem 1.
   - 1.2. Dostawa macierzy typu Rack wraz z wykonaniem usługi montażu i konfiguracji w serwerowni Zamawiającego zgodnie z załącznikiem 2.
   - 1.3. Instalacji oprogramowania serwera w tym migracji środowiska serwerowego w serwerowni Zamawiającego zgodnie z załącznikiem 5.
   - 1.4. Dostawa licencji
     - 1.4.1. Windows Server 2022 Standard 4 szt. Licencji CAL w ilości 50 szt. dla użytkowników oraz licencji CAL w ilości 15 szt. dla urządzeń.
     - 1.4.2. Z uwagi na posiadane przez Zamawiającego oprogramowanie, wymaga się od Wykonawcy, aby serwery dostarczone zostały z licencjami Microsoft Windows Server 2022 std.

2. Szczegółowy opis przedmiotu zapytania ofertowego:
   - 2.1. Przedmiotem zamówienia jest dostawa i budowa nowej infrastruktury Data Center (określanego w dalszej części niniejszego dokumentu jako „**System**") **wraz z usługą migracji** istniejącego środowiska Zamawiającego na dostarczany System
3. Przedmiot zamówienia obejmuje: realizację następujących etapów:
   - 3.1. **Etap 1** – dostawa i uruchomienie infrastruktury technicznej dedykowanej wraz z dostarczeniem licencji na oprogramowanie tworzące System. Wykonawca dostarczy, skonfiguruje i uruchomi sprzęt, okablowanie oraz oprogramowanie niezbędne do zapewnienia stabilnego działania Systemu, jego wysokiej wydajności i zgodności z obowiązującymi przepisami prawa. Dostawa dotyczyć może zarówno nowego sprzętu, oprogramowania i licencji, jak i nowych lub dodatkowych komponentów. Licencje powinny umożliwiać uruchomienie wirtualizacji na dostarczanych serwerach fizycznych i obejmować pełne wykorzystanie procesorów i pamięci operacyjnej.

   - 3.2. **Etap 2** – uruchomienie środowiska testowego, końcowa konfiguracja Systemu,
     Wykonawca uruchomi środowisko testowe poprzez przeniesienie środowiska wdrożeniowego do infrastruktury Zamawiającego. Wykonawca w sposób uzgodniony z

Zamawiającym na etapie Projektu Technicznego Wdrożenia wykona ostateczną konfigurację Systemu na środowisku testowym posiadającym pełną oczekiwaną funkcjonalność wskazaną w Opisie Przedmiotu Zamówienia (Klaster wraz z usługa migracji) tak aby umożliwić Zamawiającemu szczegółową weryfikację wdrożonego Systemu,

3.2.1. Wykonawca wykona konfiguracje klastra Hyper-V. W skład zadania wchodzić będzie konfiguracja zasobów dyskowych serwerów, macierzy i konfiguracja klastra HA

3.2.2. Wykonawca dokona migracji obecnie posiadanego środowiska Zamawiającego opartego na środowisku wirtualizacyjnym Hyper-V do nowo utworzonego klastra Hyper-V . W skład zadania wchodzi migracja wirtualnych maszyn, wirtualizacja serwera z systemem obiegu dokumentów.

3.3. **Etap 3** – uruchomienie środowiska produkcyjnego, dostawa dokumentacji technicznej Systemu, dostawa instrukcji obsługi Systemu.
Wykonawca wniesie korekty wynikające z audytu oraz testów przeprowadzonych przez Zamawiającego i uruchomi środowisko produkcyjne Systemu. Wykonawca wykona ostateczną konfigurację, testy i uruchomienie środowiska produkcyjnego Systemu spełniającego całość wymagań wskazanych w Opisie Przedmiotu Zamówienia. Wszelkie prace związane z instalacją i uruchomieniem elementów infrastruktury technicznej muszą zostać wcześniej uzgodnione z Zamawiającym i będą realizowane w ramach godzin pracy Zamawiającego. Realizacja tych prac nie mogą kolidować z działaniem innych systemów użytkowanych przez Zamawiającego

3.4. **Etap 4** – Wykonawca zrealizuje szkolenie z wdrożonych rozwiązań w siedzibie Zamawiającego po zakończeniu prac. Czas trwania szkolenia nie mnie niż 4 godzin. W zakres szkolenia wchodzi administracja środowiska wirtualnego.

Infrastruktura techniczna Systemu

Wykonawca zobowiązany jest do dostarczenia oraz skonfigurowania i uruchomienia takich elementów infrastruktury technicznej, aby wypełnić wymagania postawione przed Systemem
Na potrzeby Systemu przewiduje się zastosowanie dwóch serwerów fizycznych oraz macierzy w jednym budynku wraz z wymaganymi w OPZ licencji, oraz wykonaniem usługi konfiguracji środowiska wirtualnego opartego o wymagany w postępowaniu wirtualizator Microsoft Hyper-V.
Jeżeli do osiągnięcia wszystkich zakładanych celów wdrożenia Systemu (funkcjonalnych, wydajnościowych, niezawodności) niezbędne okaże się zastosowanie również jakichś innych elementów infrastruktury technicznej, to Wykonawca zobowiązany jest do ich dostarczenia i uruchomienia. W tym przypadku wszystkie wymagania dotyczące opisanej w tym dokumencie infrastruktury technicznej mają zastosowanie również do tych dodatkowych elementów, w szczególności wymóg, że Zamawiający nie dopuszcza uruchamiania jakichkolwiek funkcjonalności bezpośrednio na serwerach fizycznych, bez zastosowania wirtualizacji niezgodnej z Projektem Technicznym Wdrożenia.

Serwer szt. 2

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.4GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 229 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	- minimum jeden slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 porty 10/25GbE SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dodatkowa karta: Karta SAS do podłączenia urządzeń zewnętrznych
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB, 6Gb, 2,5" Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10
System operacyjny/dodatkowe oprogramowanie	Zainstalowany Windows Server 2022 Standard (licencja musi zostać dobrana tak aby przy zaproponowanych procesorach umożliwić uruchomienie min. 4 maszyn wirtualnych) **Dodatkowo należy dostarczyć:** 1x nośnik do downgrade-u do wersji Windows Server 2019 Standard (wystarczy jeden nośnik na całe proponowane rozwiązanie)

	1x nośnik do downgrade-u do wersji Windows Server 2016 Standard (wystarczy jeden nośnik na całe proponowane rozwiązanie) Oprogramowanie Microsoft Windows Server 2022 User CAL – 50 sztuk Oprogramowanie Microsoft Windows Server 2022 Device CAL – 15 sztuk
Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;

	• integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Warunki gwarancji	3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 8x5 poprzez ogólnopolską linię telefoniczną producenta. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera Dostawca musi posiadać: Dedykowany portal chmurowy do zgłaszania awarii lub usterek zabezpieczony protokołem SSL Możliwość logowania się do systemu z przeglądarki Firefox, Chrome, safari, opera, edge, internet Explorer Logowanie do systemu za pomocą loginu: własnego adresu e-mail i hasła, które użytkownik może samodzielnie zmienić System musi mieć możliwość dodania minimum 100 urządzeń System musi mieć możliwość przypisania do urządzenia - numeru seryjnego sprzętu - minimum 2 numerów wewnętrznych potrzebnych do wewnętrznej identyfikacji oraz inwentaryzacji sprzętu System musi posiadać możliwość generowania kodów QR dla danego produktu uwzględniając jego numer seryjny do zgłaszania usterek poprzez SMS lub Strefę Klienta W panelu klienta użytkownik musi mieć możliwość zobaczyć wykaz urządzeń wraz z numerem seryjnym oraz numerami wewnętrznymi W panelu klienta użytkownik musi mieć możliwość zgłoszenia usterki urządzenia wybierając konkretne urządzenie W panelu klienta musza znajdować się wszystkie zgłoszenia oraz musi być możliwość ich filtracji po numerze seryjnym, modelu lub marce urządzenia

Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.

Macierz dyskowa szt. 1

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do instalacji w standardowej szafie RACK 19", macierz musi zajmować maksymalnie 2U i pozwalać na instalacje 12 dysków 3.5".
Kontrolery	Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów SAS 12Gbit
Kable/wkładki	Wraz z macierzą należy dostarczyć komplet minimum 4 sztuk okablowania umożliwiającego podłączenie do oferowanych serwerów sygnowanych logiem producenta.
Cache	16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii.
Dyski	Zainstalowane: 8 dysków Hot-Plug o pojemności 4TB SAS, 3 dyski Hot-Plug o pojemności 960GB SSD SAS Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 264 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
Oprogramowanie/Funkcjonalności	Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN'ów oraz 1024 kopii migawkowych na całą macierz. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków. Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 8TB poprzez dyski SSD. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym.
Wsparcie dla systemów operacyjnych/wirtualizatorów	Windows Server 2022, 2019 and 2016 RHEL 8.2 and 7.8 SLES 15.2 and 12.5

	VMware 7.0 and 6.7 Citrix Xen 8.x and 7.x VMware vSphere (ESXi) vCenter; SRM Microsoft Hyper-V
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
Warunki gwarancji dla macierzy	3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. • Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. • Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu. • W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych). Dostawca musi posiadać: Dedykowany portal chmurowy do zgłaszania awarii lub usterek zabezpieczony protokołem SSL Możliwość logowania się do systemu z przeglądarki Firefox, Chrome, safari, opera, edge, internet Explorer Logowanie do systemu za pomocą loginu: własnego adresu e-mail i hasła, które użytkownik może samodzielnie zmienić System musi mieć możliwość dodania minimum 100 urządzeń System musi mieć możliwość przypisania do urządzenia - numeru seryjnego sprzętu - minimum 2 numerów wewnętrznych potrzebnych do wewnętrznej identyfikacji oraz inwentaryzacji sprzętu System musi posiadać możliwość generowania kodów QR dla danego produktu uwzględniając jego numer seryjny do zgłaszania usterek poprzez SMS lub Strefę Klienta

	W panelu klienta użytkownik musi mieć możliwość zobaczyć wykaz urządzeń wraz z numerem seryjnym oraz numerami wewnętrznymi W panelu klienta użytkownik musi mieć możliwość zgłoszenia usterki urządzenia wybierając konkretne urządzenie W panelu klienta musza znajdować się wszystkie zgłoszenia oraz musi być możliwość ich filtracji po numerze seryjnym, modelu lub marce urządzenia
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty	Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2015.

Usługa wdrożenia:

1. Wykonawca wykona fizyczną instalację i podłączenie okablowania zasilające i komunikacyjnego w serwerowni Zamawiającego następujące urządzenia:
   - 2 serwery opisane w OPZ
   - macierz opisana w OPZ
   - dostawa i instalacja pamięci dedykowanej 16 GB RAM do serwera Dell R240
2. Wykonawca uruchomi i skonfiguruje zainstalowany sprzęt:
   - aktualizacja firmware i oprogramowanie systemowe do bieżącej wersji (urządzenia powyżej)
   - nadanie adresacji IP wg dokumentacji Zamawiającego
   - konfiguracja modułów zarządzających serwerów
   - konfiguracja grup dyskowych: SSD – RAID1, SAS – RAID5
   - utworzenie wolumenów logicznych i nadania uprawnień hostom
3. Instalacja środowiska wirtualnego i konfiguracja klastra HA
   - instalacja Windows Server 2022 Standard na dostarczanych serwerach z usługą Hyper-V
   - podłączenie do hostów wolumenów dostarczanej macierzy
   - Konfiguracja usługi HA dla utworzonego klastra
   - migracja 2 maszyn wirtualnych z serwera posiadanego przez Zamawiającego
   - wirtualizacja posiadanego przez Zamawiającego serwera obiegu dokumentów do klastra HA, opartego o system operacyjny Linux. Ilość danych ok. 2TB
4. Wykonawca wykona rekonfigurację domeny do obsługi profili mobilnych:
   - utworzenie grupy AD dla użytkowników mobilnych
   - utworzenie polityk GPO z limitami „Quote” dla wskazanych przez Zamawiającego folderów dla profili użytkowników mobilnych
   - utworzenie profili mobilnych dla 50 użytkowników
   - Wykonawca pilotażowo nadzoruje logowanie do profili mobilnych 10 wskazanych użytkowników
5. Po migracji Wykonawca przeprowadzi rekonfigurację posiadanego przez Zamawiającego serwera
   - instalacja zapasowego kontrolera domeny i podłączeni do istniejącej domeny Zamawiającego
   - instalacja czystej maszyny wirtualnej z rolą serwera plików i podłączenie do domeny
6. Instalacja i konfiguracja systemu backupu posiadanego przez Zamawiającego
   - przygotowanie serwera jako hosta dla maszyn wirtualnych systemu backupu

- przygotowanie zadań backupu dla 5 maszyn wirtualnych zgodnie z polityką backupu
- testy odtworzeniowe dla wybranych maszyn

7. Dokumentacja wdrożeniowa
   - Wykonawca przygotuje i przekaże Zamawiającemu dokumentację dla całego zakresu zrealizowanego wdrożenia
8. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego
   - sesja szkoleniowa będzie trwała do 8 godzin
   - zakres szkolenia administratorów będzie obejmował obsługę klastra Hyper-V i obsługę systemu backup
9. Zamawiający wymaga wsparcia powdrożeniowego w wymiarze minimum 8h w okresie 2 miesięcy

IX. Pozostałe elementy zamówienia

10. Ponadto Wykonawca w cenie oferty zobowiązuje się ująć koszty m.in.:
    1) Wykonania i umieszczenia naklejek na potrzeby oznakowania każdego urządzenia zgodnie z zasadami promocji i oznakowania projektów w Programie Polska Cyfrowa w szczególności zgodnie z Kartą wizualizacji Programu Polska Cyfrowa na lata 2014-2020 - wg. załącznika nr 2 do OPZ.
11. Forma wynagrodzenia ryczałtowego (art. 632 KC) wymaga od Wykonawcy również wyceny ryzyka, bowiem Wykonawca nie będzie mógł żądać zmiany wynagrodzenia ryczałtowego dla zakresu dostaw objętych niniejszym zamówieniem.
12. Wykonawca jest odpowiedzialny za staranne zaznajomienie się z dokumentacją przetargową.
13. Wykonawca przed zawarciem umowy przedłoży Zamawiającemu kosztorys ofertowy w formie uproszczonej.
14. RODO: Dane osobowe Wykonawcy dostaw, podwykonawców oraz dane zawarte w dokumentacji powykonawczej będą przechowywane przez cały okres trwania gwarancji.

Załącznik nr 1

Opis kryteriów równoważnych

***System operacyjny**

System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   – Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   – Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
2. Funkcje związane z obsługą komputerów typu przenośnego, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego
3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
9. Wbudowany system pomocy w języku polskim.
10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.

***Oprogramowanie – pakiet biurowy**

1. Wymagania odnośnie interfejsu użytkownika:

- Pełna polska wersja językowa interfejsu użytkownika
- Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych
- Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

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

- posiada kompletny i publicznie dostępny opis formatu,
- ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych(Dz.U.05.212.1766)
- umożliwia wykorzystanie schematów XML
- wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)

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:

- Edytor tekstów
- Arkusz kalkulacyjny
- Narzędzie do przygotowywania i prowadzenia prezentacji
- Narzędzie do tworzenia i wypełniania formularzy elektronicznych
- Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)

7. Edytor tekstów musi umożliwiać:

- Edycję i formatowanie tekstu w języku polskim, angielskim i niemieckim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej orazfunkcjonalnością słownika wyrazów bliskoznacznych i autokorekty

- Wstawianie oraz formatowanie tabel
- Wstawianie oraz formatowanie obiektów graficznych
- Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
- Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
- Automatyczne tworzenie spisów treści
- Formatowanie nagłówków i stopek stron
- Sprawdzanie pisowni w języku polskim
- Śledzenie zmian wprowadzonych przez użytkowników
- Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
- Określenie układu strony (pionowa/pozioma)
- Wydruk dokumentów
- Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
- Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007, 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
- Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
- 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.
- Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.

8. Arkusz kalkulacyjny musi umożliwiać:

- Tworzenie raportów tabelarycznych
- Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
- Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
- Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
- Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
- Wyszukiwanie i zamianę danych

- Wykonywanie analiz danych przy użyciu formatowania warunkowego
- Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
- Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
- Formatowanie czasu, daty i wartości finansowych z polskim formatem
- Zapis wielu arkuszy kalkulacyjnych w jednym pliku
- Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń
- Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

9.

9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

- Przygotowywanie prezentacji multimedialnych, które będą:
  - Prezentowanie przy użyciu projektora multimedialnego
  - Drukowanie w formacie umożliwiającym robienie notatek
  - Zapisanie jako prezentacja tylko do odczytu.
- Nagrywanie narracji i dołączanie jej do prezentacji
- Opatrywanie slajdów notatkami dla prezentera
- Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
- Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
- Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
- Możliwość tworzenia animacji obiektów i całych slajdów
- Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
- Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010, 2013 i 2016.
- Przesłanie danych przy użyciu usługi Web (tzw. web service).
- Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.
- Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jeg wypełnienia.

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

- Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
- Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
- Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
- Automatyczne grupowanie poczty o tym samym tytule
- Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
- Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
- Zarządzanie kalendarzem
- Udostępnianie kalendarza innym użytkownikom
- Przeglądanie kalendarza innych użytkowników
- Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
- Zarządzanie listą zadań
- Zlecanie zadań innym użytkownikom
- Zarządzanie listą kontaktów
- Udostępnianie listy kontaktów innym użytkownikom
- Przeglądanie listy kontaktów innych użytkowników
- Możliwość przesyłania kontaktów innym użytkowników.
- Możliwość przesyłania kontaktów innym użytkowników.

Zał. nr 2 do OPZ Naklejka na sprzęt 72x18_Naklejka_fundusze_cyfrowa_gmina-1

UWAGA!

Naklejka o wymiarach min. 5 cm x 7 cm, wykonana na foli odpornej na działanie promieni UV, umieszczona w widocznym miejscu na sprzęcie.