Szczegółowy opis przedmiotu zamówienia

zamówienia na dostawę sprzętu komputerowego w celu poprawy bezpieczeństwa cyfrowego w Starostwie Powiatowym w Słubicach oraz zwiększenia zakresu cyfryzacji pracy dofinansowaną w ramach powierzonego grantu o numerze 5515/P/2022 w Programie Operacyjnym Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji konkursu grantowego „Cyfrowy Powiat" o numerze POPC.05.01.00-00-0001/21-00

Zamawiający dopuszcza składanie ofert częściowych z podziałem na 3 następujące części:

1) **Część 1** – **dostawa urządzenia do ochrony sieci – firewall (jednego urządzenia)** fabrycznie nowego, tzn. nieużywanego przed dniem dostarczenia, pochodzących z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych,
2) **Część 2** – **dostawa urządzenia wielofunkcyjnego A3 i urządzenia wielofunkcyjnego A4**, tj. jednego urządzenia wielofunkcyjnego A3 i jednego urządzenia wielofunkcyjnego A4 - fabrycznie nowych, tzn. nieużywanych przed dniem dostarczenia, pochodzących z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych,
3) **Część 3** – **dostawa komputerów przenośnych**, których to zakres rzeczowy obejmuje dostawę **11 szt.** notebooków (z oprogramowaniem biurowym) - fabrycznie nowych, tzn. nieużywanych przed dniem dostarczenia, pochodzących z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych,

wraz z transportem do siedziby Zamawiającego i wniesieniem do wskazanego miejsca/pomieszczenia. Wykonawca ponadto dostarczy wraz z zamówieniem wymaganej do obsługi instrukcji w języku polskim oraz dostarczy dokumentację techniczną, użytkową związaną z przedmiotem zamówienia.

Część 1 – dostawa urządzenia do ochrony sieci - firewall

Wymagania minimalne
Oferowany sprzęt ma być fabrycznie nowy, nieużywany oraz nieeksponowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, wyprodukowany nie wcześniej niż w 2022 r., a także musi spełniać wymagania techniczno-funkcjonalne, jakościowe i funkcjonalne wyszczególnione w poniższym opisie przedmiotu zamówienia.

Urządzenie do ochrony sieci - firewall	
Nazwa	**Minimalne wymagania dla sprzętu**
Zastosowanie	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	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: • 16 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 2 gniazdami SFP+ 10 Gbps. 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 co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 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 2.5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
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 Stateful Inspection. 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 - 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. 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 także dla protokołu HTTP/2. 12. Analiza ruchu szyfrowanego protokołem SSH. 13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
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: 3. Translację jeden do jeden oraz jeden do wielu. 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 7. 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 • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.
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/Counter Mode(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.	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

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. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
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 Safe Search – 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 url - 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. 4. 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 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 lub EAL4 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: 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 36 miesięcy.
Warunki gwarancji	System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Ilość	1 szt.

Załącznik Nr 2 do zapytania ofertowego

Część 2 – dostawa urządzenia wielofunkcyjnego A3 i urządzenia wielofunkcyjnego A4

Wymagania minimalne

Oferowany sprzęt ma być fabrycznie nowy, nieużywany oraz nieeksponowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, wyprodukowany nie wcześniej niż w 2022 r., a także musi spełniać wymagania techniczno-funkcjonalne, jakościowe i funkcjonalne wyszczególnione w poniższym opisie przedmiotu zamówienia.

Urządzenie wielofunkcyjne kolorowe A3	
Nazwa	**Minimalne wymagania dla sprzętu**
Charakterystyka kopiarki	
Prędkość kopiowania	Min. 35 stron A4/min kolor i mono
Rozdzielczość kopiowania	Min. 2400 dpi x 600 dpi
Pamięć	Min. 4 GB RAM
Dysk twardy	Min. 320 GB
Format oryginału	od A5 do A3
Format kopii	od A5 do A3
Czas nagrzewania	Max. 15 sekund
Czas pierwszej kopii	Max. 10 sekund
Kopiowanie ciągłe	od 1 do 999
Gramatura papieru	Min. 64– 280 g/m2
Natężenie obrazu	automatyczne i ręczne
Zoom	25% do 400% , w krokach, co 1 %
Inne funkcje	tryb foto, auto wybór papieru, auto przełączanie podajników papieru , auto start, kierunkowa zmiana rozmiaru, rotacja obrazu, sortowanie elektroniczne
Kody dostępu dla użytkowników	Min. 999 kodów
Podajniki na papier	Min. Trzy uniwersalne zasobniki na papier od A5 do A3 na min. 3200 arkuszy 80 g/m2
Obsługa	Min. Kolorowy panel LCD 10,1 cala w języku polskim
Dupleks	Min. od A5 do A3 o gramaturze 60-256 g/m2
Automatyczny podajnik oryginałów typu DSDF	Min. 300 arkuszy 80 g/m2
Dodatkowy zasobnik na papier	Min. zasobnik na papier A4, min. 2500 arkuszy 80 g/m2
Gniazdo USB	Bezpośrednie drukowanie z nośników
Finiszer wewnętrzny	Min. dwie tace odbiorcze, pojemność min. 600 arkuszy, zszywanie wielopozycyjne do 50 arkuszy A4R-A3, 60-105 g/m2
Charakterystyka drukarki	
Prędkość	Min. 35 strony A4 /min kolor i mono
Jakość druku	Min. 3600 dpi x1200 dpi
Pamięć	Min. 4 GB RAM
Języki opisu strony	Min. XPS, PCL6 i PostScript3
Interfejs	USB 2.0 High Speed
Zgodne systemy operacyjne	Windows 8/7/Vista/XP/Server 2008, Server 2003 (32/64 bity)/Windows Server2008 R2(64 Bity), Mac OS X 10.4.11-10.8,Linux/Unix, Citrix, Novel Netware (NDPS), SAP, AS/400
Karta sieciowa	Ethernet 10/100 BaseTX
Charakterystyka skanera	
Prędkość skanowania	Min. 240 skanów A4/min /mono i kolor
Formaty plików	JPG, wielostronicowy/jednostronny TIFF, XPS/PDF, Slim PDF, zabezpieczony PDF, , przeszukiwany PDF, edytowanie plików DOC, XLS, RTF, TXT
Typ oryginałów	tekst, foto, tekst+foto,
Rozmiar oryginałów	od A5 do A3
Rozdzielczość	Min. 600 dpi, kolor (8 bit) lub mono
Warunki gwarancji	– Minimum 24 miesięczna gwarancja producenta door to door. – Czas reakcji serwisu - do końca następnego dnia roboczego. – Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta
Ilość	1 szt.

Załącznik Nr 2 do zapytania ofertowego

dostawa urządzenia wielofunkcyjnego A4

Wymagania minimalne

Oferowany sprzęt ma być fabrycznie nowy, nieużywany oraz nieeksponowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, wyprodukowany nie wcześniej niż w 2022 r., a także musi spełniać wymagania techniczno-funkcjonalne, jakościowe i funkcjonalne wyszczególnione w poniższym opisie przedmiotu zamówienia.

Urządzenie wielofunkcyjne kolorowe A4	
Nazwa	**Minimalne wymagania dla sprzętu**
Charakterystyka kopiarki	
Prędkość kopiowania	Min. 38 stron A4/min kolor i mono
Rozdzielczość kopiowania	2400 dpi x 600 dpi
Pamięć	Min. 4 GB RAM
Dysk twardy	Min. 320 GB
Format oryginału	od A6 do A4
Format kopii	od A6 do A4
Czas nagrzewania	Max. 14 sekund
Czas pierwszej kopii	Max. 7 sekund
Kopiowanie ciągłe	od 1 do 999
Gramatura papieru	Min. 64– 218 g/m2
Natężenie obrazu	automatyczne i ręczne
Zoom	25% do 400% , w krokach, co 1 %
Inne funkcje	tryb foto, auto wybór papieru, auto przełączanie podajników papieru , auto start, kierunkowa zmiana rozmiaru, rotacja obrazu, sortowanie elektroniczne
Kody dostępu dla użytkowników	Min. 999 kodów
Podajniki na papier	Min. trzy uniwersalne zasobniki na papier od A6 do A4 na min. 1200 arkuszy 80 g/m2
Obsługa	Min. Kolorowy panel LCD 7 cali w języku polskim
Dupleks	Min. A4 o gramaturze 52-120 g/m2
Automatyczny podajnik oryginałów	Min. 50 arkuszy 80 g/m2
Gniazdo USB	Bezpośrednie drukowanie z nośników
Charakterystyka drukarki	
Prędkość	Min. 38 stron A4 /min kolor i mono
Jakość druku	Min. 1200 dpi x1200 dpi
Pamięć	Min. 4 GB RAM
Języki opisu strony	Min. XPS, PCL6 i PostScript3
Interfejs	USB 2.0 High Speed
Zgodne systemy operacyjne	Windows 8/7/Vista/XP/Server 2008, Server 2003 (32/64 bity)/Windows Server2008 R2(64 Bity), Mac OS X 10.4.11-10.8,Linux/Unix, Citrix, Novel Netware (NDPS), SAP, AS/400
Karta sieciowa	Ethernet 10/100 BaseTX
Charakterystyka skanera	
Prędkość skanowania	Min. 55 skanów A4/min /mono i kolor
Formaty plików	JPG, wielostronicowy/jednostronny TIFF, XPS/PDF, Slim PDF, zabezpieczony PDF, , przeszukiwany PDF, edytowanie plików DOC, XLS, RTF, TXT
Typ oryginałów	tekst, foto, tekst+foto,
Rozmiar oryginałów	od A6 do A4
Rozdzielczość	Min. 600 dpi, kolor (8 bit) lub mono
Warunki gwarancji	– Minimum 24 miesięczna gwarancja producenta door to door. – Czas reakcji serwisu - do końca następnego dnia roboczego. – Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta
Ilość	1 szt.

Załącznik Nr 2 do zapytania ofertowego

Część 3 – dostawa komputerów przenośnych

Wymagania minimalne

Oferowany sprzęt ma być fabrycznie nowy, nieużywany oraz nieeksponowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, wyprodukowany nie wcześniej niż w 2022 r., a także musi spełniać wymagania techniczno-funkcjonalne, jakościowe i funkcjonalne wyszczególnione w poniższym opisie przedmiotu zamówienia.

Komputer przenośny - notebook	
Nazwa	**Minimalne wymagania dla sprzętu**
Matryca	A) minimum 15,6” FHD 1920 x 1080 LED B) jasność minimum 250 cd/m2
Wydajność	Procesor musi osiągać w teście wydajności PassMark - CPU Benchmarks (na dzień 18.08.2023) wynik min. 13 000 punktów według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php (wynik testu oceniany będzie według załącznika nr 1 do SOPZ - TABELA Z PARAMETRAMI WARTOŚCI PassMark - CPU Benchmarks). W ofercie wymagane podanie producenta i modelu procesora oraz wynik ww. teście na dzień 18.08.2023
Płyta główna	Zaprojektowana i wyprodukowana na zlecenie producenta komputera
Pamięć RAM	Minimum 16GB, możliwość rozbudowy do min. 32GB,
Pamięć masowa	– Minimum 512 GB SSD PCIe 4.0 NVMe – Dysk twardy musi zawierać partycję recovery – Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania.
Kamera	Wbudowana w obudowę komputera i wyposażona w migawkę, minimum 1.0 Mpix HD.
Karta dźwiękowa	Zintegrowana, dostępne gniazdo słuchawek i mikrofonu, wbudowane minimum głośniki stereo.
Karty sieciowe	Karta sieciowa minimum 10/100/1000 Ethernet, zintegrowana z płytą główną, WiFi minimum 802.11 ax/ac/a/b/g/n, Bluetooth minimum 5.0.
Porty komunikacyjne	– minimum 1 x HDMI – minimum 1 x RJ45 – minimum 4 x USB typu A (z czego minimum 1 port USB 3.2) – minimum 1 x czytnik kart SD
Wymagania dodatkowe	– Komputer musi posiadać dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – Komputer musi posiadać możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera. – W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane. Wykonawca niebędący producentem oferowanego sprzętu nie może samodzielnie dokonywać jego modyfikacji.
Bezpieczeństwo	– Komputer musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe. – Komputer musi posiadać możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. – Udostępniona bez dodatkowych opłat, pełna wersja oprogramowania, szyfrującego zawartość twardego dysku zgodnie z certyfikatem X.509 oraz algorytmem szyfrującym AES 128bit, współpracującego z wbudowaną sprzętową platformą bezpieczeństwa. – TPM minimum 2.0
System operacyjny	Zainstalowany system operacyjny spełniający następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Licencja bezterminowa. 2. Polska wersja językowa. 3. System operacyjny powinien być dostarczony w najnowszej oferowanej przez producenta wersji.

	4. Aktualizacje funkcji dla systemu operacyjnego. 5. Obsługa procesorów wielordzeniowych. 6. Graficzny okienkowy interfejs użytkownika. 7. Obsługa co najmniej 8 GB RAM. 8. Dostęp do aktualizacji w ramach zaoferowanej wersji systemu operacyjnego przez Internet bez dodatkowych opłat. 9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych: – lupa powiększająca zawartość ekranu, – narrator odczytujący zawartość ekranu, – regulacja jasności i kontrastu ekranu, – możliwość odwrócenia kolorów np. biały tekst na czarnym tle, – poprawa widoczności elementów ekranu np. regulowanie grubości kursora myszy - małej strzałki na ekranie, wskazującej lokalizację myszy i czasu trwania powiadomień systemowych, – funkcja sterowania myszą z klawiatury numerycznej, – funkcja klawiszy trwałych, która sprawia, że skrót klawiszowy jest uruchamiany po naciśnięciu jednego klawisza, – korzystanie z wizualnych rozwiązań alternatywnych wobec dźwięków, – funkcja napisów w treściach wideo, – możliwość skorzystania z wizualnych rozwiązań alternatywnych wobec dźwięków; 13. Możliwość zarządzania stacją roboczą poprzez polityki. 14. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 15. Wsparcie dla min. Sun Java i .NET Framework 1.1 i 2.0 i 3.0 i 4.5 – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 16. Wsparcie dla min. JScript i VBScript - możliwość uruchamiania interpretera poleceń. 17. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 18. Graficzne środowisko instalacji i konfiguracji. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników. 20. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 21. Oprogramowanie dla tworzenia kopii zapasowych, automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 22. Możliwość przywracania plików systemowych. 23. Możliwość identyfikacji sieci komputerowych, do których jest podłączony komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
Dodatkowe oprogramowanie	Pakiet biurowy MS Office 2021 lub równoważny, w polskiej wersji językowej, zawierający min: Word, Excel, Power Point, Outlook (lub równoważne), z licencją nieograniczoną czasowo wraz z unikatowym kluczem do aktywacji każdego dostarczonego pakietu. Wymagana pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet biurowy powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa. Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim. Pakiet musi mieć publicznie znany cykl życia przedstawiony przez producenta, dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa – co najmniej na 2 lata od daty zakupu. **Przy czym, równoważność** będzie oceniana w zakresie posiadania przez zaproponowane oprogramowanie, oprócz istotnych zbliżonych cech i parametrów do produktu referencyjnego, które muszą umożliwiać pełną obsługę wszystkich istniejących dokumentów Zamawiającego, wytworzonych przy użyciu oprogramowania Microsoft Office: 2003, 2007, 2010, 2013, 2016, 2019 (pliki tekstowe, dokumenty, arkusze kalkulacyjne zawierające makra i formularze, prezentacje itp.) bez utraty

	jakichkolwiek ich parametrów i cech użytkowych, również następujących szczegółowych funkcjonalności: 1.dla edytora tekstu MS Word 2021: a) podział okna roboczego na kilka dokumentów b) edytor rysunków c) wykonywanie korespondencji seryjnej bazującej na danych adresowych pochodzących np. z arkusza kalkulacyjnego d) wstawianie tabel i wykresów z arkusza kalkulacyjnego, w tym tabel przestawnych e) otwieranie plików PDF i edytowanie ich zawartości 2. dla arkusza kalkulacyjnego MS Excel 2021: a) ustawianie obszaru wydruku b) ręczne rysowanie obramowania c) automatyczne dopasowanie wielkości komórek do zawartości d) obsługa makr e) obsługa co najmniej 2 tys. kolumn f) tworzenie raportów tabelarycznych g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywane czynności h) tworzenie wykresów linowych (wraz z linią trendu), słupkowych, kołowych 3. dla programu do prezentacji MS Power Point 2021: a) ustawianie rozdzielczości prezentacji b) prowadzenie prezentacji w trybie prezentera - slajdy widoczne na jednym monitorze lub projektorze, a na drugim monitorze widoczne notatki prezentera 4. dla programu pocztowego Outlook 2021: a) obsługa i praca na plikach danych Outlook (pst) b) wbudowany kalendarz c) obsługa zadań i spotkań Zamawiający wymaga, aby licencja na dostarczony pakiet biurowy nie była wcześniej aktywowana na innym sprzęcie komputerowym. Obsługa plików pst wymagana m.in. celem zachowania ciągłości korespondencji e-mail użytkowników komputerów (obecna forma przechowywania e-maili). Zainstalowanie oprogramowania biurowego na jednym komputerze pochodzącego więcej niż od jednego producenta nie będzie uznane za „pakiet biurowy”. Zamawiający zastrzega sobie możliwość zwrócenia się do oferenta o nieodpłatne dostarczenie proponowanego oprogramowania równoważnego w wersji testowej czy na licencji ograniczonej czasowo, jeśli nie jest ono dostępne powszechnie w sieci, celem oceny równoważności względem produktu referencyjnego.
Certyfikaty	– Certyfikat ISO 9001 dla producenta sprzętu – Certyfikat ISO 14001 dla producenta sprzętu – Deklaracja zgodności CE – Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.
Warunki gwarancji	– Minimum 36 miesięczna gwarancja producenta door to door. – Czas reakcji serwisu - do końca następnego dnia roboczego. – Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera
Ilość	11 szt.

TABELA Z PARAMETRAMI WARTOŚCI PassMark - CPU Benchmarks (ze strony: http://www.cpubenchmark.net na dzień 18.08.2023 r.) STANOWI ZAŁĄCZNIK DO SOPZ.