Burmistrz Zelowa

Urząd Miejski w Zelowie
ul. Żeromskiego 23
97-425 Zelów
www.zelow.pl
umzelow@zelow.pl

tel. 44/ 634 10 00
tel. 44/ 634 10 03
fax 44/ 634 13 41

Fundusze Europejskie Program Regionalny

promuje łódzkie

Unia Europejska Europejski Fundusz Społeczny

ZPI. 271.33.2020

Zelów, 17.08.2020r.

„Dostawa sprzętu komputerowego w ramach projektu pt.: „Podnoszenie kompetencji edukacyjnych w gminie Zelów" realizowanego w ramach RPO Województwa Łódzkiego współfinansowanego przez Unię Europejską w ramach środków Europejskiego Funduszu Społecznego".

W związku z art. 38 ust.4 ustawy Prawo zamówień publicznych, który stanowi, iż „W uzasadnionych przypadkach zamawiający może przed upływem terminu składania ofert zmienić treść specyfikacji istotnych warunków zamówienia. Dokonaną zmianę treści specyfikacji zamawiający udostępnia na stronie internetowej, chyba że specyfikacja nie podlega udostępnieniu na stronie internetowej…". - Zamawiający zmienia treść załącznika nr 6 do SIWZ w pkt. 4 i 5. Zmieniony załącznik nr 6 w załączeniu.

wz. BURMISTRZA
mgr Anetta Mądry
ZASTĘPCA BURMISTRZA

Załącznik nr 6 do SIWZ

Dostawa sprzętu komputerowego w ramach projektu pt. „Podnoszenie kompetencji edukacyjnych w gminie Zelów" realizowanego w ramach RPO Województwa Łódzkiego współfinansowanego przez Unię Europejską w ramach środków Europejskiego Funduszu Społecznego.

lp	nazwa	ilość	szczegółowy opis	producent/model/kod producenta oraz szczegółowa specyfikacja sprzętu- **wypełnia wykonawca**	stawka podatku VAT	cena jedn. brutto	wartość ogółem brutto w PLN
	2	3	4	5	6	7	8
	Laptop z oprogramowaniem	66	Minimalne wymagania: **I. Komputer przenośny** 1. Typ: komputer przenośny 2. Monitor/ wyświetlacz: TFT LCD, min. 15,6" 3. Rozdzielczość matrycy: min. Full HD 1920 x 1080 4. Wydajność obliczeniowa procesora: w teście Passmark - CPU Mark wg. wyników procesorów publikowanych na stronie http://www.cpubenchmark.net/cpu_list.php procesor uzyskujący wynik co najmniej 7.900 punktów 5. Wydajność obliczeniowa karty graficznej: w teście Average G3D Mark wg. wyników publikowanych na stronie https://www.videocardbenchmark.net/gpu_list.php karta uzyskująca wynik co najmniej 1200 punktów 6. Pamięć operacyjna: min. 8 GB 7. Parametry pamięci masowej: dysk SSD min. 512 GB SSD 8.Wyposażenie multimedialne: zintegrowana karta dźwiękowa, wbudowany mikrofon, wbudowane głośniki stereo 9. Wymagania dodatkowe: - Łączność: moduł Bluetooth, Wi-Fi 802.11 ac, zintegrowany z płytą LAN 1000 Mbps - Rodzaje wejść/wyjść: porty USB - min. 3 szt. (w tym min. 2 w wersji wyższej niż 2.0), Wyjście słuchawkowe/wejście mikrofonowe (osobno lub combo) - 1 szt., HDMI - 1 szt., RJ-45 - 1 szt. 10. Oprogramowanie: najnowszy stabilny system operacyjny, zainstalowany przez producenta, z interfejsem dostępnym w kilku językach do wyboru: minimum w polskim i angielskim, w pełni obsługujący najnowszy zestaw funkcji API wspomagających generowanie grafiki, dźwięku oraz innych zadań związanych z aplikacjami multimedialnymi oraz umożliwiający zarządzanie wersjami plików poprzez kopie w tle, zalecany Windows 10 PL. Zamawiający nie dopuszcza wersji edukacyjnych				
			II. Oprogramowanie biurowe Minimalne wymagania: Najnowsze stabilne oprogramowanie biurowe z wieczystą licencją na urządzenie, spełniające następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji zawierające następujące elementy: edytor tekstu, arkusz kalkulacyjny, program do prezentacji, program do obsługi bazy danych w pełni wspierający formaty Open XML, jak również narzędzie do zarządzania informacją prywatą: pocztą elektroniczną, kalendarzem, kontaktami i zadaniami. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). Tworzenie raportów z zewnętrznych źródeł danych, którymi mogą być inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice. Oprogramowanie powinno mieć zapewnione wsparcie techniczne Producenta				

			III. Oprogramowanie antywirusowe Minimalne wymagania: Antywirus Musi oferować kompleksową ochronę klienta / serwerów poprzez ochronę sieci korporacyjnych przed wirusami , trojanami, robakami , hakerami, wirusami sieciowymi , zagrożeniem ataku z wielu punktów wejścia i plikami typu spyware. Mają zdolność do wykrywania wszystkich wirusów, a silnik antywirusa powinien posiadać certyfikat VB100%, OPSWAT, AVLAB +++ Musi posiadać zdolność do wykrywania i blokowania plików ze szkodliwą zawartością i osadzonych / skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji Musi posiadać zdolność do wykrywania i usuwania plików typu rootkit Musi posiadać zdolność do wykrywania szkodliwych plików i przeprowadzenia kwarantanny Musi posiadać zdolność do wykrywania złośliwego oprogramowania za pomocą technik wykrywania behawioralnych Musi posiadać zdolność do wykrywania i usuwania fałszywego oprogramowania bezpieczeństwa (roguewear) Musi posiadać zdolność do identyfikacji źródła zainfekowanych plików w sieci Musi mieć zdolność do przywracania plików z kwarantanny, jeśli plik jest zakwalifikowany jako bezpieczny Musi posiadać mechanizm zapobiegający rozprzestrzenianiu wirusa aktywowany już na etapie wykrycia wirusa Powinien wykrywać szkodliwy typ oprogramowań i je usuwać Zwykli użytkownicy nie powinni mieć możliwość modyfikowania ustawień AV za wyjątkiem grup specjalnych ustawionych przez administratorów Menadżer aktualizacji : musi posiadać możliwość tworzenia wielu serwerów aktualizacji rozpowszechniania aktualizacji Musi posiadać funkcje skanowania skompresowanych, spakowanych oraz zarchiwizowanych plików Musi posiadać funkcje skanowania telefonu podłączonego do komputera i usuwania z niego zagrożeń Musi posiadać funkcje skanowania urządzeń USB zaraz po ich podłączeniu Musi być zdolny do określania i usuwania wszelkich zagrożeń stworzonych przez wirusy typu Trojan Musi posiadać funkcje odłączenia zainfekowanej końcówki od siec Musi posiadać funkcje skanowania i naprawiania plików OLE. Musi posiadać funkcje odłączenia zainfekowanej końcówki od sieci w przypadku wykrycia podejrzanych/zawirusowanych plików w pamięci Musi posiadać funkcję skanowania ruchu https Musi skanować kontenery skrzynek mailowych Musi mieć możliwość skanowanie plików zarchwizowanych Musi mieć możliwość określania poziomu zagnieżdżenia skanowania oprogramowania antywirusowego Musi mieć możliwość wybrania typu akcji w przypadku wykrycia wirusa w archiwum Musi mieć możliwość akcji w przypadku znalezienia wirusa Musi oferować rozpoznawanie zagrożeń na podstawie zachowań behawioralnych Musi zapewniać wykluczenie ze skanowania określonych plików, folderów oraz plików o zadanym rozszeżeniu Musi posiadać możliwość chronienia systemy użytkownika przed nowymi zagrożeniami typu Ransoware.						

			Program musi posiadać możliwość wygenerowania raporty dotyczącego działań typu Ransomware. Program musi mieć możliwość automatycznego tworzenia kopi zapasowych plików a potem przywracania tych danych po ataku Program musi mieć możliwość dodawania wykluczeń do aplikacji lub katalogu aplikacji, które nie będą skanowane w poszukiwaniu zagrożeń. Musi posiadać harmonogram skanowania Musi posiadać możliwość konfiguracji wszystkich funkcji antywirusa przy zadaniu skanowania z harmonogramu Musi posiadać funkcjonalność powtarzania skanowania w określonych interwałach czasu np. co 1 godzinę Musi zapewniać skanowanie zewnętrznych urządzeń Musi posiadać funkcje automatycznego skanowania zewnętrznych urządzeń Musi zrobić kopię pliku przed próbą naprawy pliku Musi posiadać funkcję ochrony urządzeń mobilnych podłączonych poprzez USB i Bluetooth Ochrona e-mail Musi zapewniać ochronę poczty e-mail Musi blokować wysyłanie e-mail utworzonych przez zagrożenia exploitowe Musi mieć możliwość blokowania załączników Musi mieć możliwość określonych rozszerzeń w załącznikach Musi mieć możliwość blokowania wszystkich załączników Musi zapewniać skanowanie poczty w protokołach szyfrowanych SSL Musi zapewniać ochronę antywirusowa podczas startu systemu operacyjnego Musi posiadać funkcję ochrony zaufanych klientów pocztowych takich jak Microsoft Outlook Express, Microsoft Outlook, Eudora, i Netscape Navigator Musi posiadać filtr anty SPAM Musi mieć możliwość ustawienia czułości filtra anty SPAM Musi mieć możliwość dodawania białych oraz czarnych list adresów e-mail do filtra anty SPAM Ochrona IPS/IDS Musi posiadać moduł ochrony IDS/IPS Musi posiadać mechanizm wykrywania skanowania portów Moduł wykrywania skanowania portów musi mieć możliwość określenia kilku poziomów wrażliwości Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów Musi posiadać moduł wykrywania ataków DDoS Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania ataków Ddos Musi mieć możliwość blokowania atakującego na określony czas Musi mieć możliwość odłączania końcówki która wykonuje ataki DDoS i Port scanning Musi wyświetlać komunikat w przypadku wykrycia ataku DDoS i Port Scanning Firewall Musi zapewnić elastyczność w tworzeniu reguł zapory filtrowania połączeń na podstawie adresu IP , numeru portu lub protokołu , a następnie zastosować te zasady do różnych grup użytkowników				

			Musi mieć możliwość kontroli i nadzoru nad całym ruchem wchodzącym i wychodzącym Musi posiadać predefiniowane poziomy ochrony firewall Musi posiadać predefiniowane reguły firewall gotowe do użycia Musi posiadać dodatkową kontrole połączeń WiFi Musi mieć możliwość wyświetlania ostrzeżeń w przypadku zagrożenia wykrytego przez firewall Musi mieć możliwość włączania i wyłączania raportów w module firewall Musi mieć możliwość dodawania nowych reguł firewall Reguły firewal muszą pozwalać na określanie zakresów adresów IP, portów TCP/IP oraz protokołów TCP UDP ICMP Musi umożliwiać dodanie wyjątków Firewall za pomocą adresów IP lub nazw DNS (URL) Ochrona przeglądania Musi posiadać możliwość zablokowania użytkownikowi dostępu do zainfekowanych i phishingowych stron internetowych ze skonfigurowanych punktów końcowych Musi posiadać możliwość zablokowania dostępu do stron w oparciu o ich kategorie Musi posiadać możliwość blokowania całej domeny lub witryny Musi posiadać możliwość wykluczenia domen stron internetowych lub całych domen Musi posiadać możliwość zablokowania połączenia HTTPS Musi mieć możliwośc blokowania określonych domen i sub domen Musi posiadać możliwość określania czasu w którym końcówki mają dostęp do stron internetowych Musi posiadać możliwość dodania wyjątku z blokady czasowej dostępu do stron internetowych Musi posiadać możliwość dodawania wykluczeń z filtra kategorii Skaner podatności Musi posiadać skaner podatności Musi posiadać możliwość wyboru czy skanowane mają być produkty firmy Microsoft, produkty firm trzecich czy też oba warianty naraz Skaner podatności musi posiadać swój harmonogram Raport skanera podatności powinien zawierać, datę i czas wykonania skanowania, nazwę końcówki, domenę/grupę roboczą, numer CVE podatności, nazwę podatności, poziom zagrożenia, producenta W raporcie powinny być wyświetlane zagrożone platformy, linki do opisu problemu oraz opis szczegółowy podatności Informacje o danej podatności muszą mieć możliwość drukowania oraz generowania do PDF i CVS Zarządzanie aktywami Musi posiadać moduł zarządzania aktywami na końcówkach Musi informować o nazwie komputera Musi informować o nazwie domeny/ grupy roboczej Musi informować o szczegółach systemu operacyjnego w tym nazwie systemu operacyjnego, wersji systemu operacyjnego, typie systemu operacyjnego, producent systemu operacyjnego Musi informować o kluczu systemu operacyjnego Musi informować o istniejących lokalnych kontach użytkowników Musi informować które lokalne konta użytkowników są włączone a które wyłączone Powinien informować o dacie i godzinie uruchomienia komputera Powinien informować o dacie i godzinie ostatniego restartu komputera Powinien informować o producencie komputera					
1									

			Powinien informować o modelu komputera Powinien informować o nr. seryjnym płyty głównej komputera Powinien informować o rodzaju, modelu i producencie procesora zainstalowanego w komputerze Powinien informować o częstotliwości pracy procesora Powinien informować o ilości pamięci RAM fizycznej oraz wirtualnej Powinien informować o zainstalowanych dyskach twardych, partycjach, typie systemu plików, pojemności oraz wolnej przestrzeni dyskowej Powinien informować o producencie, wersji i dacie BIOS'u Powinien informować o zainstalowanych kartach grafiki Powinien informować o zainstalowanych kartach dźwiękowych Powinien informować o zainstalowanych wszystkich interfejsach sieciowych Informacje o interfejsach sieciowych powinny zawierać, nazwę połączenia, adres fizyczny MAC, czy adres pobierany jest z serwera DHCP, adres IPv4, adres IPv6, maskę sieci, bramę domyślną , serwery DNS, informacje czy włączony jest NetBIOS przez TCP IP Powinien wyświetlać informację o monitorze zainstalowanym na końcówce Powinien informować o drukarkach zainstalowanych sieciowo i lokalnie Powinien informować o zainstalowanych aplikacjach na komputerze końcówce Powinien móc informować kto jest producentem zainstalowanego oprogramowania, w jakiej wersji jest zainstalowane oprogramowanie oraz kiedy oprogramowanie było zainstalowane Musi mieć możliwość generowania raportów z zarządzani aktywami do formatu CVS Musi mieć możliwość wykonania raportu w każdej chwili i na końcówce wybranej przez administratora Inne funkcje Musi móc odtwarzać ustawienia przeglądarki Internet Explorer po udanym ataku malware Musi móc usuwać pozostawione ślady aktywności aplikacji i przeglądarek internetowych Musi mieć możliwość stworzenia awaryjnego dysku do naprawy zainfekowanego systemu Musi mieć możliwość uruchomieni tylko skanowania antymalwerowego Musi mieć możliwość ochrony pamięci usb przed auto uruchamianiem Musi posiadać moduł za zarządzania uruchomionymi procesami systemowymi Musi posiadać "szpiega aplikacji" w którym wskazujemy uruchomiona aplikacje i otrzymujemy raport zawierający: ścieżkę do aplikacji, nazwę aplikacji, oryginalna nazwę pliku, wersje pliku i dane producenta Ze "szpiega systemu" musi być możliwość zamknięcia procesu Dostęp do ustawień oprogramowania musi być chroniony hasłem Program powinien zapewniać ochronę trybu awaryjnego systemu windows dodatkowo chronioną hasłem Musi obsługiwać funkcje Sandbox dla bezpiecznego przeglądania Musi zapewniać bezpieczne wykonywanie operacji bankowych W przypadku podnoszenia wersji oprogramowania serwerowego, powinien być dostępny tryb migracji wielo serwerowej Klient EPS musi umożliwiać podgląd informacji o serwerze do którego jest podłączony Zaawansowana kontrola urządzeń				

			Musi posiadać różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie Musi posiadać funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD ... Musi posiadać funkcje regulowania połączeń WiFi i Bluetooth Musi być zdolny do zachowania kontroli nad interfejsami programów typu: SATA controller, Thunderbolt itd Musi posiadać funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu : drukarki, skanery i kamery internetowe Musi posiadać funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi Musi posiadać funkcje blokowania dostępu dowolnemu urządzeniu Musi posiadać funkcje odłączenia dowolnego urządzenia na podstawie nazwy modelowej Musi mieć zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym klientem EPS Musi posiadać możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka Musi posiadać możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora Musi posiadać możliwość zarządzani urządzeniami podłączanymi do końcówki takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry Musi posiadać możliwość używania tylko zaufanych urządzeń sieciowych w tym urządzeń wskazanych na końcówkach klienckich Musi posiadać możliwość wysyłania informacji do producenta Musi posiadać możliwość dodawania urządzeń magazynowych USB za pomocą numeru seryjnego bez podłączania Musi posiadać funkcję wirtualnej klawiatury Konsola Administracyjna Konsola administracyjna musi korzystać z technologii MS IIS System raportujący powinien korzystać z bazy danych typu SQL Generowanie paczek instalacyjnych dla końcówki musi mieć możliwość wyboru czy paczka jest dla systemu 32 czy 64 bitowego, czy ma być w wersji exe czy msi dla systemu windows Podczas generowania paczki musi mieć możliwość wyboru paczki pełnej oraz minimalnej z częściową instalacja z internetu Przy generowaniu paczki dla systemu linux musi mieć wybór systemu 32 i 64 bitowego 1. Musi posiadać możliwość instalowania oprogramowania klienckiego przy użyciu : 1.1 Client Packer (Microsoft installer) 1.2 Strony instalacyjnej na serwerze lokalnym 1.3 Zdalna instalacja na pojedynczym punkcie końcowym lub w całym zakresie IP				

			1.4 Z obrazu dysku klienta 1.5 Poprzez Active Directory oraz stworzenie grupy Musi zapewnić bezpieczny graficzny interfejs użytkownika lub konsoli zarządzania opartej o sieć w celu zapewnienia administratorom dostępu do wszystkich klientów i serwerów w sieci Powinien posiadać strukturę administracji opartą na przypisywaniu ról użytkownikom Musi posiadać funkcje dostarczania wiadomości SMS lub E-mail w przypadku zdarzeń krytycznych Musi posiadać zdolność do tworzenia raportów tabelarycznych i graficznych Musi posiadać możliwość eksportowania raportów w wielu formatach conajmniej CSV i PDF Musi posiadać możliwość automatycznego wysyłania raportu do administratorów zgodnie z harmonogramem Musi posiadać możliwość automatycznego czyszczenia starych raportów Musi posiadać możliwość do logowania wszystkich aktywność serwera zarządzania Musi umożliwiać instalację klienta z obrazu dysku Musi umożliwiać zdalną deinstlacje oprogramowania na końcówce Każda funkcjonalność musi posiadać dedykowany panel raportowania Każda funkcjonalność musi posiadać możliwość konfiguracji w każdej z polityk Architektura serwera musi wspierać do 5000 punktów końcowych Architektura zarządzania musi umożliwiać tworzenie pod-serwerów Musi umożliwiać tworzenie administratorów ograniczonych do zarządzania wybranymi grupami Musi wyświetlać statystyki niezaktualizowanych klientów w zakresach 1, 3, 7, 15 i 30 dni Musi umożliwiać centralne wycofanie aktualizacji z wybranych komputerów końcowych na wypadek wadliwej aktualizacji Musi umożliwiać automatyczną aktualizację serwera zarządzania za pomocą paczek aktualizacji Musi posiadać możliwość integracji konsoli z rozwiązaniem szyfrowania dysków Musi posiadać panel informacji o licencji w tym podział na pod-serwery oraz posiadane licencje DLP Wspierane systemy operacyjne Musi wspierać co najmniej: Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit) Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit) Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit) Microsoft Windows 7 Home Basic/ Premium / Professional / Enterprise / Ultimate (32-bit/64-bit) Microsoft Windows Vista Home Basic/ Premium / Business / Enterprise / Ultimate (32-bit/64-bit) Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit / 64-bit) Microsoft Windows Server 2019 (64-bit) Microsoft Windows Server 2016 Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit) Microsoft Windows MultiPoint Server 2012 Standard (64-bit) Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)				

			Microsoft Windows SBS 2011 Standard / Essentials Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit) Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit) Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit) Mac Mac OS X 10.9, 10.10, 10.11 macOS 10.12, 10.13, 10.14, 10.14.5 Linux 32 bity RHEL 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 BOSS 6 Fedora 14, 18, 19, 20, 21, 22, 23, 24, 25 openSUSE 11.4, 12.2, 12.3, 13.2, 42.2 Linux Mint 13, 14, 15, 16, 17.3, 18 Ubuntu 10.10, 11.4, 12.04 LTS, 12.04.3 LTS, 13.04, 13.10, 14.04, 14.10, 15.04, 16.04 LTS, 16.10, 17.04 CentOS 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 Linux 64 bity RHEL 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2, 7.3 Fedora 14, 18, 19, 20, 21, 22, 23, 24, 25 openSUSE 11.4, 12.2, 12.3, 42.3 Linux Mint 13, 14, 15, 16, 17.3, 18 Ubuntu 10.10, 11.4, 12.04.2 LTS, 13.04, 13.10, 14.04, 14.10, 15.04, 16.04 LTS, 16.10, 17.04 CentOS 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0 SUSE Linux 11.00, 12.00, 12.2				
						Razem	

cenę netto i brutto należy przenieść do formularza ofertowego	W przypadku zastosowania przez dostawcę na proponowane towary stawki podatku VAT, innej niż podstawowa tj. 23% należy wypełnić poniższe zestawienie:		
kolumnę 5,6,7,8,wypełnia wykonawca	poz.	objęte stawką podatku VAT	podać podstawę prawną .....

wz. BURMISTRZA
mgr Aneta Mądry
ZASTĘPCA BURMISTRZA