**Załącznik nr 2.**

**Szczegółowy opis przedmiotu zamówienia / Oferowane parametry techniczne sprzętu**

Dostaw sprzętu komputerowego i oprogramowania w ramach projektu Cyfrowa Gmina.

1. Przedmiotem zamówienia jest: Zakup sprzętu komputerowego i oprogramowania w ramach projektu „Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU”.

2. Przedmiot zamówienia został podzielony na 4 cześci :

**Część 1. Zakup serwera w ramach projektu „Cyfrowa Gmina”,** w zakres której wchodzi dostawa:

* 1. Serwer główny – 1 szt.

**Część 2. –** **Zakup sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina**”, w zakres której wchodzi dostawa:

2.1 Urządzenie zapory sieciowej typu UTM z wdrożeniem – 1 szt.

**Część 3. – Zakup sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina”, w zakres której wchodzi dostawa:**

3.1 Komputer stacjonarny typu All In One – 6 szt.

3.2 Komputer przenośny laptop typu netebook - 1 szt.

**Część 4. – Zakup sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina”, w zakres której wchodzi dostawa:**

4.1 Zasilacz awaryjny do komputera stacjonarnego (UPSY) - 18 szt.

4.2 Oprogramowanie MS Office 2019 Home&Business PL – 22 szt.

4.3 Urządzenie do uwierzytelniania dla systemów operacyjnych i aplikacji dziedzinowych – 20 szt.

4.4 Oprogramowanie do szyfrowania – 20 szt.

4.5 Urządzenie do backup – 1 szt.

Niniejszy załącznik stanowi jednocześnie szczegółowy opis przedmiotu zamówienia. Zaoferowany przez Wykonawcę sprzęt komputerowy i oprogramownie musi spełniać minimalne wymagania postawione w niniejszym załączniku w kolumnie „Wymagane minimalne parametry techniczne ” oraz zostać dostarczony na warunkach określonych poniżej. Wykonawca w kolumnie „Oferowane parametry techniczne TAK/NIE\*” winien odnieść się do każdego z wymagań minimalnych postawionych przez Zamawiającego w kolumnie „Wymagane minimalne parametry techniczne ” i dokonać zaznaczenia prawidłowej odpowiedzi TAK LUB NIE . Wykonawca zobowiązany jest podać też producenta, model oferowanego sprzętu , typ. Dodatkowo Zamawiający dopuszcza podanie linków dostępowych dla oferowanego n/w sprzętu dostępnych na stronach internetowych producentów.

Wykonawca może złożyć ofertę na wszystkie cztery części zamówienia lub na dowolnie wybraną część zamówienia.

* 1. **Serwer główny – 1 szt.**

|  |  |  |
| --- | --- | --- |
| Parametr | Opis | Oferowane parametry techniczne  Producent…………….  Model………………….  Typ…………………….. |
| Obudowa | Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. | TAK/NIE\* |
| Płyta główna | Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | TAK/NIE\* |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych | TAK/NIE\* |
| Procesor | Jeden procesor 6-rdzeniowy, min. 3.5GHz, umożliwiający osiągnięcie wyniku min. 57.3 w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org w konfiguracji jednoprocesorowej. | TAK/NIE\*  UZUPEŁNIĆ: (Procesor)  Producent …………….  Model …………………..  Liczba punktów……………….. |
| Pamięć RAM | 128GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s.  Na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci | TAK/NIE\* |
| Karta graficzna | Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 | TAK/NIE\* |
| Wbudowane porty | min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, min. 1 port RS232 | TAK/NIE\* |
| Gniazda PCI | Min. 3 sloty PCIe generacji 4 | TAK/NIE\* |
| Interfejsy sieciowe/FC/SAS | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT  Dodatkowa 4 portowa karta 1Gb Ethernet BaseT | TAK/NIE\* |
| Kontroler dysków | Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED. | TAK/NIE\* |
| Dyski twarde | Możliwość instalacji dysków SAS, SATA, SSD, NL SAS  Zainstalowane 4 dyski NLSAS o pojemności min. 2TB, 12Gb, Hot-Plug.  Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug 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. | TAK/NIE\* |
| System operacyjny/ wirtualizator | Windows 2019 lub 2022 - Windows 2022 Datacenter •    Licencje dostępowe CAL o    20 x Device lub User CAL Wbudowany napęd DVD +/- RW | TAK/NIE\* |
| Diagnostyka | Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. | TAK/NIE\* |
| Wentylatory | Minimum 4 wentylatory | TAK/NIE\* |
| Zasilacze | Redundantne, o mocy maks. 600W. | TAK/NIE\* |
| 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 | TAK/NIE\* |
| Diagnostyka | Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. | TAK/NIE\* |
| 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 | TAK/NIE\* |
| Gwarancja | 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 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.  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. | TAK/NIE\* |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001 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 2019, Windows Server 2022. | TAK/NIE\* |
| Dokumentacja | 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. | TAK/NIE\* |

**Część 2. –** **Zakup sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina**”, w zakres której wchodzi dostawa:

2.1 Urządzenie zapory sieciowej typu UTM z wdrożeniem – 1 szt.

|  |  |  |
| --- | --- | --- |
| Parametr | Opis wymagań minimalnych | Oferowany parametry techniczne  Producent…………….  Model………………….  TAK/NIE |
| Wymagania Ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. | TAK/NIE |
| Redundancja, monitoring i wykrywanie awarii | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.  Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  Monitoring stanu realizowanych połączeń VPN.  System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. | TAK/NIE |
| Interfejsy, Dysk, Zasilanie: | System realizujący funkcję Firewall musi dysponować minimum:  5 portami Gigabit Ethernet RJ-45.  System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej xxx interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.  System musi być wyposażony w zasilanie AC. | TAK/NIE |
| Parametry wydajnościowe: | W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.  Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.  Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.  Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.  7. 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.  8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.  9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps. | TAK/NIE |
| 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. 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 | TAK/NIE |
| Polityki, Firewall | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  Translację jeden do jeden oraz jeden do wielu.  Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.  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. | TAK/NIE |
| Połączenia VPN | 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.  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. | TAK/NIE |
| 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. | TAK/NIE |
| Funkcje SD-WAN | System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.  Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. | TAK/NIE |
| Zarządzanie pasmem | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.  System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. | TAK/NIE |
| Ochrona przed malware | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.  System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  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.  System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.  Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. | TAK/NIE |
| Ochrona przed atakami | Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.  Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.  System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  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.  Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | TAK/NIE |
| Kontrola aplikacji | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. | TAK/NIE |
| Kontrola WWW | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  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.  Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.  Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.  Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.  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 | 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.  Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.  Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.  Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | TAK/NIE |
| Zarządzanie | 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.  Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.  Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.  System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.  System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. | TAK/NIE |
| 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. | TAK/NIE |
| Certyfikaty | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. | TAK/NIE |
| Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [12] miesięcy. | TAK/NIE |
| Gwarancja oraz wsparcie | 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres [12] 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. | TAK/NIE |
| Rozszerzone wsparcie serwisowe AHB/SOS | System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [12] miesięcy.  b)Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5 przedłożyć dokumenty: • Zamawiający powinien dostarczyć oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego. | TAK/NIE |
| Wdrożenie | Wdrożenie podstawowe obejmuje:  -Aktywacja Licencji  -Aktualizacja Firmware  -Instalacja Dimension i ustawienie przesyłania logów z Firebox  -Konfiguracja klastra Active-Passive/Active-Active  -Konfiguracja kont administracyjnych  -Konfiguracja interfejsów sieciowych  -Konfiguracja Multi-WAN (Failover)  -Konfiguracja DNS, NTP  -Konfiguracja DNAT  -Konfiguracja DHCP  -Konfiguracja mVPN (SSL, IKEv2)  Uruchomienie oraz konfiguracja modułów bezpieczeństwa:  -Network Discovery  -Geolokalizacja  -IPS  -App Control  -WebBlocker  -spamBlocker  -Gateway AntiVirus  -Reputation Enabled Defense (RED)  -IntelligentAV  -APT Blocker  -Access Portal  -Konfiguracja globalnych polityk bezpieczeństwa dla protokołów:  #DNS  #NTP  #FTP  #HTTP  #HTTPS  #POP3  #IMAP  #SMTP | TAK/NIE |

**Część 3. –** **Zakup sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina**”, w zakres której wchodzi dostawa:

3.1 Komputer stacjonarny typu All In One – 6 szt.

3.2 Komputer przenośny laptop typu netebook - 1 szt.

* 1. **Stacje robocze - Komputer stacjonarny All in One – 6 sztuk**

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne komputerów | Parametry  Spełnia:  (Proszę zaznaczyć odpowienie)  TAK/NIE  Producent:…………………  Model:………………………  Numer katalogowy (numer  konfiguracji lub part numer):……………………... |
| Ekran | Przekątna: min 23,5”  Rozdzielczość: min. FHD (1920x1080) IPS lub WVA lub MVA, matowa, podświetlenie LED, 250nits, kąty widzenia min. 170 stopni w pionie i poziomie. Wielkość pojedynczego pixela nie większa niż 0,28mm | TAK/NIE |
| Obudowa | * zintegrowana z monitorem (AIO) * musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona lub równoważne pozwalające na fizyczne zabezpieczenie urządzenia) * Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością demontażu stopy. * Obudowa trwale oznaczona nazwą producenta, nazwą komputera, part numberem, numerem seryjnym * Podstawa musi umożliwiać regulację kąta pionie w zakresie -5 do 25 stopni oraz w poziomie -45 do +45 stopni | TAK/NIE |
| Chipset | Dostosowany do zaoferowanego procesora | TAK/NIE |
| Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera  Wyposażona w min. 2 złącza M.2 z czego jedno obsługujące dysk SSD PCIe NVMe | TAK/NIE |
| Procesor | Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych osiągający liczbę punktów minimum 10.040 na poziomie wydajności liczonej w punktach na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. | TAK/NIE  UZUPEŁNIĆ: (Procesor)  Producent …………….……….  Model ……………………………  Liczba punktów………………………… |
| Pamięć operacyjna | min. 8 GB SODIMM DDR4  Ilość banków pamięci: min. 2 szt. | TAK/NIE |
| Dysk twardy | Min 256 GB, umożliwiający odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. | TAK/NIE |
| Napęd optyczny | Nie wymagany | TAK/NIE |
| Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci. | TAK/NIE |
| Audio/Video | Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo 2 x 3W, wbudowany mikrofon, wbudowana kamera 1080p z wbudowaną przesłoną mechaniczną umożliwiającą jej fizyczne zasłonięcia.  Możliwość podłączenia zewnętrznego monitora wraz ze wsparciem rozdzielczości 4K w min. 30Hz. | TAK/NIE |
| Karta sieciowa | LAN 10/100/1000 Mbit/s z funkcją Wake on LAN  WiFi 1x1 AC + Bluetooth min. 5.0 | TAK/NIE |
| Porty/złącza | Wbudowane (minimum): HDMI-in, HDMI-out, 5 x USB typu A z czego min. 2 x USB3.1, 1x USB-C, 1 x RJ 45 (LAN), 1 x wyjście na słuchawki/wejście na mikrofon (combo), czytnik kart pamięci min 3w1. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. | TAK/NIE |
| Klawiatura/mysz | Klawiatura przewodowa w układzie US. Mysz przewodowa z rolką (scroll) | TAK/NIE |
| Zasilacz | Zasilacz o sprawności minimum 88% o mocy nie większej niż 130W. | TAK/NIE |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych  2. Funkcje związane z obsługą komputerów typu tablet, 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.  16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".  17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.  18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.  23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."  24. Wbudowany mechanizm wirtualizacji typu hypervisor."  25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.  26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).  29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.  30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.  31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM  33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.  34. Możliwość tworzenia wirtualnych kart inteligentnych.  35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)  36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.  37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.  38. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty inteligentne i certyfikaty (smartcard),  c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  d. Certyfikat/Klucz i PIN  e. Certyfikat/Klucz i uwierzytelnienie biometryczne  39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5  40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.  41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach  42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń | TAK/NIE |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera.  Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera, producencie komputera  - numerze seryjnym,  - numerze inwentarzowym,  - MAC Adres karty sieciowej,  - wersja Biosu wraz z datą produkcji,  - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni  - ilości pamięci RAM wraz z taktowaniem,  - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku twardego i napędu optycznego)  - o zainstalowanej licencji systemu operacyjnego na płycie głównej  Możliwość z poziomu Bios:  - wyłączenia selektywnego (pojedynczego) portów USB,  - wyłączenia selektywnego (pojedynczego) portów SATA,  - wyłączenia wbudowanej kamery, karty WiFi, karty audio, mikrofonu, głośników, czytnika kart  - włączania/wyłączania trybu PXE  - włączania/wyłączania obsługi TPM  - włączania/wyłączania wirtualizacji oraz funkcji I/O  - włączania/wyłączania funkcji Turbo procesora o ile ją obsługuje  - ustawienia hasła: administratora, Power-On, HDD,  - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan)  - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii  - zdefiniowania trzech sekwencji bootujących (podstawowa, WOL, po awarii)  - załadowania optymalnych ustawień Bios | TAK/NIE |
| Zintegrowany System Diagnostyczny | Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:   * wykonanie testu pamięci RAM * test dysku twardego wraz z możliwością wyświetlania danych SMART * test matrycy LCD * test magistrali PCI-e * test portów USB * test CPU * test myszy i klawiatury * test napędu optycznego   Wizualna sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera.  Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:   * Komputer: Producent, PN, model * BIOS: Wersja oraz data wydania Bios * Procesor: ilość rdzeni, wątków, obsługiwane instrukcje i pamięć cache * Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci * Dysk twardy: model, numer seryjny, wersja firmware, pojemność, prędkość obrotowa, temperatura pracy * LCD: producent, model, rozmiar, rozdzielczość * Napęd optyczny: producent, wspierane nośniki/tryby zapisu   System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. | TAK/NIE |
| Certyfikaty i standardy | * Certyfikat ISO9001 dla producenta sprzętu * Energy Star * Deklaracja zgodności CE * EPEAT min. Silver * Ochrona oczu (min. Low Blue Light) * Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki | TAK/NIE |
| Waga/rozmiary urządzenia | Waga urządzenia bez podstawy max. 6kg  Szerokość bez podstawy nie większa niż: 545mm | TAK/NIE |
| Bezpieczeństwo i zdalne zarządzanie | Złącze typu Kensington Lock  Możliwość ustawienia portów USB w jednym z dwóch trybów:   * użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer, ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB * użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej   Wbudowana mechaniczna zasłona obiektywu kamery. | TAK/NIE |
| Gwarancja | 1 rok świadczona w miejscu użytkowania sprzętu (on-site)  Wymagane dołączenie do oferty oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. | TAK/NIE |
| Wsparcie techniczne producenta | Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki.  Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera  Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.  Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta. | TAK/NIE |
| Wymagania dodatkowe | Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. . W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek | TAK/NIE |

* 1. **Laptop – 1 sztuka**

|  |  |  |  |
| --- | --- | --- | --- |
| Szczegółowy opis | | Parametry oferowane | |
| Komputer przenośny.  W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.  Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego.  Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający. | | Producent:…………………  Model:………………………  Numer katalogowy (numer konfiguracji lub part numer):……………………... | |
| Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 7 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek | | TAK/NIE | |
| Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.  Linki stron producenta umożliwiające weryfikacje:………………………………… | |  | |
| Nazwa komponentu | Wymagane minimalne parametry techniczne komputerów | Parametry  Spełnia:  (Proszę zaznaczyć odpowiednie)  TAK/NIE | |
| Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi 16.05 punktowana podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. | TAK/NIE  UZUPEŁNIĆ: (Procesor)  Producent …………….  Model …………………..  Liczba punktów……………….. | |
| Pamięć operacyjna RAM | Min. 16 GB dual-channel 3200MHz Możliwość rozbudowy pamięci do min. 32GB | TAK/NIE | |
| Parametry pamięci masowej | M.2 512 GB SSD PCIe NVMe  Możliwość rozbudowy do konfiguracji dwudyskowej - dostępny drugi slot M.2 na dysk SSD. | TAK/NIE | |
| Karta graficzna | Dedykowana karta o pamięci własnej minimum 4GB z pamięciami GDDR6, o wydajności liczonej w punktach równej lub wyższej 6000 pkt na podstawie PerformanceTest w teście G3DMark według wyników opublikowanych na http://www.videocardbenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. | TAK/NIE | |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby Audio stereo (2x2W), port słuchawek i mikrofonu typu COMBO, kamera video 1080p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute). |  | |
| Obudowa | Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810G.  Jako potwierdzenie parametrów wytrzymałościowych należy dostarczyć oświadczenie producenta komputera lub jego oświadczenie dotyczące oferowanego modelu. | | TAK/NIE | |
| Płyta główna | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej. | | TAK/NIE | |
| Zgodność z systemami operacyjnymi | Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera ). | | TAK/NIE | | |
| Bezpieczeństwo | TPM 2.0  Slot umożliwiający fizyczne zabezpieczenie komputera np. Kensington | | TAK/NIE | | |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). | | TAK/NIE | | |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera.  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:  - wersji BIOS  - nr seryjnym komputera  - Ilości zainstalowanej pamięci RAM  - typie procesora i jego prędkości - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS  Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:   * Możliwość ustawienia hasła Administratora * Możliwość ustawienia hasła Użytkownika * Możliwość ustawienia hasła dysku twardego * Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS * Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. * Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth | | TAK/NIE | | |
| Ekran | Matowy, matryca TFT 15” z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, 300nits, kontrast 800:1 w technologii IPS/PLS/WVA  Kąt otwarcia pokrywy ekranu min.180 stopni. | | TAK/NIE | | |
| Interfejsy / Komunikacja | Min. 2xUSB 3.2, min 1x Thunderbolt 4, złącze zasilania, złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. 2.0 umożliwiające podłączenie i obsługę ekranu w rozdzielczości 4k (3840x2160) przy 60Hz, RJ-45.Czytnik kart pamięci. | | TAK/NIE | | |
| Karta sieciowa WLAN | Wbudowana karta sieciowa, pracująca w standardzie AX 2x2  Bluetooth 5.2 | | TAK/NIE | | |
| Klawiatura | Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w 2 stopniowe podświetlanie przycisków. | | TAK/NIE | | |
| Czytnik linii papilarnych | Wbudowany czytnik linii papilarnych w przycisku zasilania | | TAK/NIE | | |
| Akumulator | Pozwalający na nieprzerwaną pracę urządzenia do min. 6 godzin – załączyć test lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 30 minut od 0% do 50% lub 60 minut od 0% do 80%. | | TAK/NIE | | |
| Zasilacz | Zasilacz zewnętrzny max. 135W | | TAK/NIE | | |
| Certyfikaty, oświadczenia i standardy | * Dla producenta sprzętu należy dostarczyć: * ISO 9001 * ISO 14001 * ISO 50001 * Komputer spełniający: * ENERGY STAR 8.0 * Mil-STD-810G * Ochronę oczu TÜV Low Blue Light * Deklaracja zgodności CE   Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki | | TAK/NIE | | |
| Waga/Wymiary | Waga urządzenia z akumulatorem nie większa niż 1,9 kg  Grubość notebooka nie większa niż: 2cm | | TAK/NIE | | |
| System operacyjny | Microsoft Windows 11 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych  2. Funkcje związane z obsługą komputerów typu tablet, 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.  16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".  17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.  18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.  23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."  24. Wbudowany mechanizm wirtualizacji typu hypervisor."  25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.  26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).  29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.  30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.  31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM  33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.  34. Możliwość tworzenia wirtualnych kart inteligentnych.  35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)  36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.  37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.  38. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty inteligentne i certyfikaty (smartcard),  c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  d. Certyfikat/Klucz i PIN  e. Certyfikat/Klucz i uwierzytelnienie biometryczne  39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5  40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.  41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach  42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń | | TAK/NIE | | |
| Oprogramowanie do aktualizacji sterowników | Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. | | TAK/NIE | | |
| Gwarancja | Minimalny czas trwania wsparcia technicznego producenta wynosi 12 miesięcy.  Firma serwisująca musi posiadać ISO 9001 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. | | TAK/NIE | | |
| Wsparcie techniczne producenta | * Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera * Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. * Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera * Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00   Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.  Należy podać link do:  - zaawansowanej diagnostyki  - do listy autoryzowanych Partnerów Serwisowych | | TAK/NIE | | |

**Część 4. –** **Zakup** **sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina**”, w zakres której wchodzi dostawa:

1) Zasilacz awaryjny do komputera stacjonarnego (UPS) - 18 szt.

2) Oprogramowanie MS Office 2019 Home&Business PL – 22 szt.

3) Urządzenie do uwierzytelniania dla systemów operacyjnych i aplikacji dziedzinowych – 20 szt.

4) Oprogramowanie do szyfrowania – 20 szt.

5) Urządzenie do backup – 1 szt.

* 1. **Zasilacz awaryjny do komputera stacjonarnego – 18 sztuk**

|  |  |  |
| --- | --- | --- |
| Parametry/Typ | Wymagania minimalne parametry techniczne. | Oferowane parametry techniczne  Producent…………….  Model…………………. |
| Moc pozorna | min. 550VA | TAK/NIE\* |
| Moc rzeczywista | min. 330W | TAK/NIE\* |
| Technologia | VI (line interactive) | TAK/NIE\* |
| Typ obudowy | wolnostojąca | TAK/NIE\* |
| Praca sieciowa | | |
| Napięcie wejściowe | 162 ÷ 290 V AC ± 7 V | TAK/NIE\* |
| Częstotliwość napięcia wejściowego | 40 ÷ 70 Hz ± 1 Hz | TAK/NIE\* |
| Zakres napięcia wyjściowego | 230 V AC ± 10 % | TAK/NIE\* |
| Kształt napięcia wyjściowego | Schodkowa aproksymacja sinusoidy / Tak jak na wejściu | TAK/NIE\* |
| Progi przełączania sieć – UPS | 162 ÷ 290 V AC ± 7 V | TAK/NIE\* |
| Czas przełączania sieć – UPS | <6ms | TAK/NIE\* |
| Praca bateryjna | | |
| Napięcie wyjściowe | ~230V ± 10% | TAK/NIE\* |
| Częstotliwość napięcia wyjściowego | 50 / 60 Hz ± 1% | TAK/NIE\* |
| Kształt napięcia wyjściowego na pracy bateryjnej | Schodkowa aproksymacja sinusoidy | TAK/NIE\* |
| Progi przełączania UPS – sieć | ~172 ÷ 280 V ± 7 V | TAK/NIE\* |
| Przeciążalność | > 110% - 1 min (wyłączenie UPS – praca sieciowa i bateryjna) | TAK/NIE\* |
| Zabezpieczenie wyjściowe przeciwzwarciowe | elektroniczne | TAK/NIE\* |
| Zabezpieczenie wyjściowe przeciążeniowe | elektroniczne | TAK/NIE\* |
| Czas podtrzymania dla obciążenia 165W | minimum 6 min | TAK/NIE\* |
| Akumulatory wewnętrzne | minimum 12V5Ah; szczelne, bezobsługowe VRLA | TAK/NIE\* |
| Pozostałe | | |
| Ilość i typ gniazd wyjściowych | minimum 2 gniazda z podtrzymaniem standardu PL (z bolcem uziemiającym) + minimum 1 gniazdo z podtrzymaniem standardu IEC 320 C13 (10 A) | TAK/NIE\* |
| Sygnalizacja | Akustyczno-optyczna  Dioda sygnalizująca minimum pracę sieciową, bateryjną, niski poziom baterii, przeciążenie, awarię  Sygnalizacja akustyczna informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu, awarii | TAK/NIE\* |
| Zimny start | Tak | TAK/NIE\* |
| Interfejs komunikacyjny | USB HID (kabel w komplecie) | TAK/NIE\* |
| Automatyczna regulacja napięcia AVR | wymagana | TAK/NIE\* |
| Waga UPS | do 4kg | TAK/NIE\* |
| Wymiary | nie większe niż: wysokość 160mm; szerokość 85mm; głębokość 255mm | TAK/NIE\* |
| Gwarancja | min 24 miesiące na elektronikę i 12 miesięcy na akumulatory; | TAK/NIE\* |
| Serwis | autoryzowany serwis producenta zlokalizowany w Polsce.  serwis realizowany w systemie door-to-door | TAK/NIE\* |
| Oprogramowanie | oprogramamowanie w języku polskim do zarządzania i monitorowania pracy UPS .  wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.  możliwość edycji nazw urządzeń na liście monitorowanych UPSów  wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer | TAK/NIE\* |
| certyfikaty producenta (załączyć do oferty) | ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań  deklaracja CE producenta sprzętu | TAK/NIE\* |
| oświadczenia / dokumenty | oświadczenie producenta o spełnieniu minimlanych wymaganych parametrów specyfikacji  karta katalogowa oferowanego sprzętu | TAK/NIE\* |

* 1. **Oprogramowanie MS office – 20 sztuk.**

|  |  |
| --- | --- |
| Oprogramowanie biurowe | Pakiet biurowy (wraz z licencją na czas nieokreślony, kluczem instalacyjnym tego oprogramowania): Microsoft Office 2019 PL lub innego oprogramowania biurowego równoważnego, zawierającego co najmniej: edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej oraz kalendarza, które charakteryzuje się następującymi cechami:  całkowicie zlokalizowany w języku polskim interfejs, system komunikatów i podręcznej kontekstowej pomocy technicznej (w tym także on-line) w pakiecie,  możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego),  możliwość zdalnej instalacji komponentów,  możliwość prowadzenia dyskusji oraz subskrypcji dokumentów w sieci z automatycznym powiadomieniem o zmianach w dokumentach, oraz publikowanie dokumentów wprost  z komponentów pakietu np. arkusza kalkulacyjnego,  w systemach pocztowych - możliwość delegacji uprawnień do otwierania, drukowania, modyfikowania i czytania załączanych dokumentów i informacji,  możliwość blokowania niebezpiecznej lub niechcianej poczty,  automatyczne przesyłanie poczty na podstawie reguł, automatyczne odpowiedzi, potwierdzanie dostarczenia do skrzynki adresata oraz potwierdzanie otwarcia poczty u adresata,  współpraca z systemem MS Exchange, w tym odbiór poczty, możliwość udostępniania kalendarza dla innych użytkowników,  wsparcie dla formatu XML w podstawowych aplikacjach,  możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich fragmentów,  automatyczne wyróżnianie i aktywowanie hyperlinków w dokumentach podczas edycji i odczytu,  możliwość automatycznego odświeżania danych pochodzących z Internetu w arkuszach kalkulacyjnych,  możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony,  możliwość zaszyfrowania danych w dokumentach i arkuszach kalkulacyjnych zgodnie ze standardem CryptoAPI,  możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych w wypadku odcięcia dopływu prądu,  prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach:.doc, .docx, xls,.xlsx, ppt, .pptx, .pps, .ppsx, w tym obsługa formatowania, wykonywanie i edycję makr oraz kodu zapisanego w języku Visual Basic for Application w plikach xls, xlsx, formuł, formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010 bez utraty danych oraz bez konieczności reformatowania dokumentów,  prawidłowe otwieranie i zapisywanie plików o formatach doc, docx, xls, xlsx, .ppt, pptx. .pps, .ppsx bez utraty parametrów i cech użytkowych zachowane wszelkie formatowanie, umiejscowienie tekstów, liczb, obrazków, wykresów, odstępy między tymi obiektami i kolorów, działające makra,  prawidłowa współpraca zapis, odczyt z plikami danych programów pocztowych w formacie .pst oraz prawidłowy import z formatu .dbx,  wszystkie komponenty oferowanego pakietu biurowego (edytor, arkusz, klient poczty, kalendarz oraz program do prezentacji) muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi,  poprawna praca w systemach operacyjnych w które może być wyposażony zamawiany zestaw, tj. 64-bitowych z rodziny Windows 7, Windows 8, Windows 8.1, Windows 11 lub równoważny,  w przypadku zaoferowanego oprogramowania równoważnego należy podać dokładną nazwę i wersję oferowanego produktu,  zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu. |

* 1. **Urządzenie do uwierzytelniania Token- 20 szt.**

|  |  |  |
| --- | --- | --- |
| Parametr | OPIS | Oferowane parametry techniczne  Producent…………….  Model…………………. |
| Uwierzytelnianie | Rozwiązanie daje możliwość uwierzytelniania przez komunikację NFC oraz przez porty USB | TAK/NIE\* |
| Obsługa protokołów | OTP, OATH HOTP, OATH TOTP, U2F, PIV i Open PGP) oraz FIDO2 | TAK/NIE\* |
| Systemy | Działa w systemach Microsoft Windows, MacOS, Linux i głównych przeglądarkach takich jak Chrome, Firefox, Safari, Edge i Opera | TAK/NIE\* |
| Typ USB | USB-A | TAK/NIE\* |
| Metody uwierzytelniania | Bez hasła, silny dwuskładnikowy, silny wieloskładnikowy | TAK/NIE\* |
| Produktywność i komunikacja | Konto Google, konto Microsoft, Salesforce.com | TAK/NIE\* |
| Certyfikaty | Certyfikat FIDO 2, Certyfikat FIDO Universal 2nd Factor (U2F) | TAK/NIE\* |
| Specyfikacje kryptograficzne | RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384 | TAK/NIE\* |
| Projekt i trwałość | Stopień ochrony IP68, odporny na zgniatanie, bez baterii, bez ruchomych części | TAK/NIE\* |
| Rodzaj urządzenia | Urządzenie FIDO HID, karta inteligentna CCID, klawiatura HID | TAK/NIE\* |

* 1. **Oprogramowanie do szyfrowania - 20 sztuk**

|  |  |  |
| --- | --- | --- |
| Parametr | Opis | Oferowane parametry techniczne  Producent…………….  Model………………….  Typ…………………….. |
| Konsola | 1. Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit oraz Microsoft Windows 7/8/10 32-bit i 64-bit.  2. Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2005, 2008, 2012.  3. Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI.  4. Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443.  5. Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish.  6. Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.  7. Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania.  8. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła.  9. Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej:  a) ilość znaków,  b) czy hasło ma zawierać wielkie litery,  c) czy hasło ma zawierać małe litery,  d) czy hasło ma zawierać cyfry,  e) czy hasło ma zawierać znaki specjalne,  f ) okres ważności,  g) ilość nieudanych logowań.  10. Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych.  11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:  a) ilość znaków,  b) czy hasło ma zawierać wielkie litery,  c) czy hasło ma zawierać małe litery,  d) czy hasło ma zawierać cyfry,  e) czy hasło ma zawierać znaki specjalne,  f ) okres ważności,  g) ilość nieudanych logowań,  h) możliwość zmiany hasła.  12. Konsola centralnego zarządzania musi gromadzić informacje o: a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych,  b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych,  c) dacie aktywacji klienta systemu szyfrowania danych,  d) statusu szyfrowania,  e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych,  f) stanie polityki,  g) wersji klienta systemu szyfrowania danych,  h) wersji systemu operacyjnego stacji roboczej,  i) użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej.  13. Konsola centralnego zarządzania musi pozwalać na wygenerowanie dla każdej zaszyfrowanej stacji płyty ratunkowej.  14. Konsola musi być dostępna z poziomu interfejsu WWW.  15. Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet.  16. Administrator musi mieć możliwość konfiguracji automatycznego szyfrowania pełnej powierzchni dysku po wykonanej instalacji oprogramowania.  17. Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych.  18. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny: a) instalacji klienta na stacji,  b) zaszyfrowania/odszyfrowania stacji,  c) wygenerowania klucza aktywacyjnego dla użytkownika,  d) administrowania kluczami szyfrującymi,  e) administrowania użytkownikami, którzy mają dostęp do stacji,  f) administrowania profilem ustawień dla użytkowników,  g) administrowania profilem ustawień dla stacji roboczych,  h) wymuszenia zmiany hasła,  i) zarządzania wieloma organizacjami z poziomu jednej konsoli. | TAK/NIE\* |
| Wymagania systemowe aplikcji klienckiej | 1. System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows Vista/7/8/10 32-bit i 64-bit oraz w środowiskach Microsoft Windows Server, 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit.  2. System musi posiadać certyfikat FIPS 140-2 Level 1 | TAK/NIE\* |
| Wymagania dotyczące uwierzytelniania | 1. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.  2. Aplikacja musi umożliwiać określenie, co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot.  3. Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file).  4. Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows.  5. Administrator musi posiadać możliwość modyfikacji ekranu logowania (Pre-boot). | TAK/NIE\* |
| Wymagania dotyczące ustawień aplikacji klienckiej | 1. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.  2. Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania.  3. Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób: a) sektor po sektorze,  b) kontener.  4. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła.  5. Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami.  6. Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail.  7. Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.  8. Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania.  9. Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.  10. Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania.  11. Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego.  12. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.  13. Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła.  14. Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.  15. Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła.  16. Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów:  a) Guttman.  b) US Department of Defence 5220.22-M (8-306. /E).  c) US Department of Defence 5220.22-M (8-306. /E, CiE).  d) Kryptograficzne losowe dane liczbowe.  17. Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.  18. Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego.  19. Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie.  20. Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji.  21. Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI. | TAK/NIE\* |
| Wymagania dotyczące szyfrowania | 1. Aplikacja musi dawać możliwość szyfrowania powierzchni dysku sektor po sektorze.  2. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.  3. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu, w którym został przerwany.  4. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania, w sytuacji gdy komputer nie jest podłączony do zasilania. Proces szyfrowania musi zostać wznowiony automatycznie, po podłączeniu zasilacza.  5. Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania:  a) AES (Rijndael).  b) Blowfish.  c) Triple DES (3DES).  6. Aplikacja musi umożliwiać współpracę z dyskami SSD.  7. Aplikacja musi umożliwiać współpracę z dyskami sprzętowo szyfrowanymi, działającymi w technologii TCG OPAL.  8. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.  9. Administrator musi mieć możliwość sprawdzenia, przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera.  10. Administrator musi mieć możliwość opcjonalnego szyfrowania niesystemowych partycji dysku. | TAK/NIE\* |
| Wymagania dotyczące sytuacji krytycznych | 1. W przypadku utraty hasła, aplikacja musi umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora.  2. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.  Licencja wieczysta | TAK/NIE\* |

* 1. **Urządzenie do backup – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| Funkcjonalność | Wymagania minimalne | Oferowane parametry techniczne  Producent…………….  Model…………………. |
| Procesor | Procesor czterordzeniowy 64biotowy o taktowaniu nie niższym niż 2.0GHz | TAK/NIE\* |
| Obudowa | Desktop | TAK/NIE\* |
| Procesor liczba rdzeni | Nie mniej niż 4 | TAK/NIE\* |
| Pamięć RAM | 4GB DDR4 z możliwością rozszerzenia do 8GB | TAK/NIE\* |
| Liczba zatok na dyski twarde | 4  Urządzenie zawiera minimum 2 dyski kompatybilne 4 TB, 3,5 cala. | TAK/NIE\* |
| Całkowita liczba gniazd pamięci | 1 | TAK/NIE\* |
| Kieszenie dysków M.2 | 2 x NVMe | TAK/NIE\* |
| Możliwość podłączenia modułu rozszerzającego | Tak | TAK/NIE\* |
| Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż: | 9 | TAK/NIE\* |
| Porty LAN | Wbudowane min. 2 x RJ-45 1GbE | TAK/NIE\* |
| Porty USB 3.2 | min. 2 | TAK/NIE\* |
| Port e-SATA | min. 1 | TAK/NIE\* |
| Zasilanie | Max. 100W | TAK/NIE\* |
| Mechanizm szyfrowania sprzętowego | Tak, min AES-NI | TAK/NIE\* |
| Wewnętrzny system plików | BTRFS, EXT4 | TAK/NIE\* |
| Obsługiwane tryby RAID | Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 | TAK/NIE\* |
| Funkcje backup | Możliwość tworzenia kopii bezpieczeństwa urządzeń pod Windows (Bare Metal), Linux oraz usług chmur publicznych, portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), serwer Apple Time Machine, backup na zewnętrzne dyski twarde, obsługa minimum 1024 migawek na folder udostępniony, obsługa minimum 65000 migawek na cały system | TAK/NIE\* |
| Darmowe aplikacje na urządzenia mobilne | Monitoring / Zarządzanie / Współdzielenie plików | TAK/NIE\* |
| Minimum obsługiwane aplikacje/usługi | Serwer plików, Serwer FTP, WebDav, Serwer WEB, Serwer kopii zapasowych, Serwer Monitoringu (min. 2 licencje bezpłatne), możliwość utworzenia klastra wysokiej dostępności z 2 identycznych urządzeń, Serwer pocztowy (min. 5 licencji w cenie) | TAK/NIE\* |
| VPN | VPN Server dla min. 40 połączeń | TAK/NIE\* |
| Gwarancja producenta | Min. 3 lata | TAK/NIE\* |

**Podsumowanie wyceny sprzętu i oprogramowania:**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp | Asortyment | Cena  jednostkowa netto | Cena  łączna netto |
| 1.1 | Serwer główny – 1 szt. |  |  |
| 2.1 | Urządzenie zapory sieciowej typu UTM z wdrożeniem – 1 szt. |  |  |
| 3.1 | Komputer stacjonarny typu All In One – 6 szt. |  |  |
| 3.2 | Komputer przenośny laptop typu netebook - 1 szt. |  |  |
| 4.1 | Zasilacz awaryjny do komputera stacjonarnego (UPSY) - 18 szt. |  |  |
| 4.2 | Oprogramowanie MS Office 2019 Home&Business PL – 22 szt. |  |  |
| 4.3 | Urządzenie do uwierzytelniania dla systemów operacyjnych i aplikacji dziedzinowych – 20 szt. |  |  |
| 4.4 | Oprogramowanie do szyfrowania – 20 szt. |  |  |
| 4.5 | Urządzenie do backup – 1 szt. |  |  |
|  | Suma netto | |  |
|  | Podatek VAT | |  |
|  | Kwota brutto | |  |

Kwoty za poszczególne części zamówienia należy przenieść do formularza ofertowego.

………………………………………….

Podpis wykonawcy