Załącznik nr 2 do SWZ

(obowiązkowy)

**FORMULARZ OFERTOWY**

**Nazwa Wykonawcy:** ..................................................................................................................................................................

**Adres Wykonawcy:** ...................................................................................................................................................................

**NIP:** ......................................................................................... **REGON:**....................................................................................

**Nr telefonu** ....................................................................................................................................................................................

**Adres e-mail:** ...............................................................................................................................................................................

(na który Zamawiający będzie przesyłać korespondencję)

***Gmina Szczytno***

***ul. Łomżyńska 3***

***12-100 SZCZYTNO***

*Nawiązując do ogłoszenia o zamówieniu po zapoznaniu się z warunkami prowadzonego postępowania w trybie podstawowym na podstawie art. 275 ust. 1 ustawy Prawo zamówień publicznych składamy ofertę na realizację zadania pn.:*

**Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”**

1. Oświadczamy, że Wykonamy dostawę **za cenę brutto** .................................................................................... **zł**

słownie złotych: ...................................................................................................................................................................,

w tym należny **podatek VAT w kwocie ……………….. zł (słownie: …………………….………)** wynikającą z następującego wyliczenia:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa asortymentu** | **J.m.** | **Ilość** | **Cena jednostkowa brutto** |
| 1 | Serwer aplikacyjny | szt. | 1 |  |
| 2 | Serwer NAS – służący do archiwizacji i backupu | szt. | 1 |  |
| 3 | Przełącznik zarządzalny | szt. | 1 |  |
| 4 | UPS – zasilacz awaryjny | szt. | 1 |  |
| 5 | Firewall UTM (Gmina) | szt. | 1 |  |
| 6 | Firewall UTM (GOPS) | szt. | 1 |  |
| 7 | Komputer stacjonarny | szt. | 38 |  |
| **Razem wartość brutto** | | | | |

**(wypełnić zgodnie z wymaganiami zamawiającego: tj. w kolumnie „Parametry oferowane” w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy oferowanego komponentu).**

**Dostawa sprzętu sieciowego i serwerów**

1. **Parametry serwera (opis)**

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | **Parametry oferowane**  **(w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)** |
| Obudowa | Obudowa RACK o wysokości maksymalnie 1U z możliwością instalacji minimum 4 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |  |
| Płyta główna | Płyta główna z możliwością zainstalowania jednego procesora lub więcej. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |  |
| Procesor | Jeden procesor 8-rdzeniowy, min. 2.6GHz częstotliwości bazowej/nominalnej, osiągający minimalne wyniki testów w konfiguracji jednoprocesorowej:  SPECrate2017\_int\_base wynik min. 60pkt  SPECrate2017\_int\_peak wynik min. 63pkt  SPECrate2017\_fp\_base wynik min. 52pkt  SPECrate2017\_fp\_peak wynik min. 56pkt  Maksymalny TDP dla procesora 65W  Wynik testu musi być opublikowany na stronie <https://www.spec.org/cpu2017/results/> w dniu złożenia oferty.  Do oferty należy załączyć wyniki testów |  |
| Pamięć RAM | Minimum 32GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s w układzie 2x16GB  Płyta powinna obsługiwać do minimum 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci. |  |
| Karta graficzna | Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 |  |
| Wbudowane porty | Minimum. 3 porty USB  Minimum 1 port VGA i 1 port RS232 |  |
| Interfejsy sieciowe LAN | Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT |  |
| Kontroler dysków | Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50 |  |
| Dyski twarde | W chwili dostawy możliwość instalacji dysków SAS, SATA, SSD, NL-SAS  Zainstalowane 2 dyski M.2 SATA o pojemności min. 240GB Hot-Plug w konfiguracji RAID 1 pod virtualizator  Zainstalowane 4 dyski SSD o minimalnych parametrach 480GB SATA 6Gb/s Read Intensive DWPD min.1 typu Hot Plug pod konfigurację Raid5  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 |  |
| Zasilacze | szt. 2 Redundantne, o mocy minimalnej 600W. |  |
| 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. |  |
| Dokumentacja | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |  |
| Warunki gwarancji | 24 miesięcy gwarancji, z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  Uszkodzony dysk pozostaje u Zamawiającego.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego autoryzowanego przedstawiciela. |  |

1. **Serwer NAS – służący do archiwizacji i backupu**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cecha** | **Wymagania minimalne** | | **Parametry oferowane (w każdym wierszu**  **należy określić typ/model/ producent/ nr**  **katalogowy)** |
| **Specyfikacja sprzętowa** | | | |
| **Procesor** | Procesor 64 bit Intel x86 4-rdzeniowy 4-wątkowy procesor o taktowaniu nie mniejszym niż 2.0 GHz |  | |
| **Procesor liczba rdzeni** | Nie mniej niż 4 |  | |
| **Pamięć RAM** | Nie mniej niż 8 GB DDR4 |  | |
| **Pamięć Flash** | Nie mniej niż 4GB |  | |
| **Liczba zatok na dyski twarde** | Minimum 4 |  | |
| **Obsługiwane dyski twarde** | 3.5" oraz 2.5" SATA oraz 2.5" SATA SSD |  | |
| **Pojemność dysków twardych** | Minimum 4 TB (minimum 4 dyski) |  | |
| **Możliwość podłączenia modułu rozszerzającego** | Tak, co najmniej 2 |  | |
| **Porty LAN 2,5 GbE** | Minimum 2 (2,5G/1G/100M/10M) |  | |
| **Przyciski** | Reset, Zasilanie |  | |
| **Typ obudowy** | RACK, 1U |  | |
| **Zasilanie** | 250W (x1), 100–240 V |  | |
| **Szyny rackowe** | Tak, w zestawie |  | |
| **Specyfikacja oprogramowania** | | |  |
| **Agregacja łączy** | Tak | |  |
| **Obsługiwane systemy plików** | Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ | |  |
| **Możliwość podłączenia karty WLAN na USB** | Tak | |  |
| **Szyfrowanie wolumenów** | Tak, min AES 256 | |  |
| **Szyfrowanie dysków zewnętrznych** | Tak | |  |
| **Zarządzanie dyskami** | Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD,  Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek | |  |
| **Wbudowana obsługa iSCSI** | Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN | |  |
| **Zarządzanie prawami dostępu** | Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników  Zarządzanie grupą użytkowników  Zarządzanie współdzieleniem w sieci  Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla pod folderów, Windows ACL | |  |
| **Obsługa Windows AD** | Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP | |  |
| **Funkcje backup** | Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, | |  |
| **Współpraca z zewnętrznymi dostawcami usług chmury** | Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box | |  |
| **Darmowe aplikacje na urządzenia mobilne** | Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android | |  |
| **Minimum obsługiwane serwery** | Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu | |  |
| **VPN** | VPN client / VPN server. Obsługa PPTP, OpenVPN | |  |
| **Administracja systemu** | Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu | |  |
| **Wirtualizacja** | Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.  Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. | |  |
| **Konteneryzacja** | Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker | |  |
| **Zabezpieczenia** | Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS | |  |
| **Możliwość instalacji dodatkowego oprogramowania** | Tak, sklep z aplikacjami; możliwość instalacji z paczek | |  |
| **Dyski twarde** | Macierz zostanie wyposażona w 4 dyski twarde 3.5” SATA 6Gb/s przystosowane do pracy z urządzeniami NAS (zapis ciągły 24/7) o pojemności min. 8 TB, prędkości 7200obr./min. Cache min. 256 MB. Dodatkowo dyski powinny posiadać parametr MTBF min. 2 mln godz. Wymaga się, aby dyski znajdowały się na liście kompatybilności dostarczanego urządzenia NAS zapewniając kompatybilność oraz wydajność. | |  |
| **Gwarancja** | 2 lata na urządzenie  2 lat gwarancji na dyski | |  |

1. **Przełącznik zarządzalny**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry techniczne oferowanego urządzenia** |
| **1** | **2** | **3** | **4** |
|  | Typ | Przełącznik sieciowy Ethernet Smart Management rack 1Gbit.  W ofercie wymagane jest podanie modelu, symbolu oraz producenta. | ……………………………………  */wpisać model, symbol, producenta urządzenia/* |
|  | Porty | 1. Minimum 48 porty 1G RJ45 10/100/1000BASE-T 2. Minimum 4 porty SFP+ z możliwością pracy 1G/10G   Porty SFP+ muszą być obsadzone wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX | ……………………………………  */wskazać ilość portów dla pkt a i b/* |
|  | Parametry fizyczne | Wysokość maksymalnie 1U, montowany w szafie typu rack 19’’ | |
|  | Pamięć | Co najmniej 512 MB SDRAM  Co najmniej 256 MB pamięci flash  Bufor pakietów co najmniej 1.5 MB  CPU ARM Cortex-A9 @ 800 MHz | ……………………………………  */wskazać wielkość pamięci DRAM i flash/* |
|  | Wielkość tablicy adresów MAC | Co najmniej 16000 | ……………………………………  */wypełnić/* |
|  | Ilość obsługiwanych sieci VLAN | Co najmniej 256 | ……………………………………  */wypełnić/* |
|  | Wydajność | * Przepustowość przełączania: min. 176 Gbit/s * Przełączanie dla pakietów: min. 130 Mpps. * Opóźnienie:   < 4.5 uSec dla 100 Mb  < 2.2 uSec dla 1000 Mb  <1.2 uSec dla 10 Gbps | ……………………………………  */wypełnić/* |
|  | Obsługa ramek Jumbo | O wielkości co najmniej 9216 bajtów | |
|  | Funkcjonalność urządzenia | * + obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad),   + obsługa protokołu SNTP,   + Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), MSTP (802.1s)   + Minimum 256 obsługiwanych sieci VLAN   + Automatyczne przydzielanie klasy urządzenia PoE w oparciu o LLDP oraz LLDP-MED.   + Minimum 50 możliwych do utworzenia list ACL,   + CoS zgodna z 802.1p   + Voice VLAN   + Minimum 509 wpisów ARP   + Możliwość przechowywania dwóch obrazów oprogramowania: aktywny I zapasowy   + Port Security   + DHCP Snooping   + Klient Radius   + Port mirroring,   + DHCP Relay,   + DoS Protection,   + ARP Attack Protection,   + Możliwość utworzenia minimum 32 statycznych wpisów w tablicy routingu | |
|  | Zasilanie | Zasilacz 230V AC wbudowany, | |
|  | Temperatura pracy | 0°C do 40°C | |
|  | Zarządzanie | WWW (GUI), SNMP Manager, cloud-based web portal | |
|  | Gwarancja | 2 lata | |

1. **UPS – zasilacz awaryjny**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry techniczne oferowanego urządzenia** |
| **1** | **2** | **3** | **4** |
|  | Typ | |  | | --- | | Bezprzerwowy zasilacz UPS | | …………………………………  */wpisać model, symbol, producenta urządzenia/* |
|  | moc | 3000 VA / 3000 W | ……………………………………  */wskazać /* |
|  | Ilość Faz | 1 + G | |
|  | Zakres napięcia | 110 VAC - 300 VAC ± 5 % (w zależności od obciążenia) | ……………………………………  */wskazać/* |
|  | Sprawność całkowita | 90 % | ……………………………………  */wypełnić/* |
|  | Obudowa | RACK maksymalnie 3 U | ……………………………………  */wypełnić/* |
|  | Czas podtrzymania | Minimum 8 minut przy obciążeniu 50% oraz 5 minut przy obciążeniu 100% | ……………………………………  */wypełnić/* |
|  | komunikacja | Port komunikacyjny RS232 i USB | |
|  | Zarządzanie | Oprogramowanie zarządzające z możliwością zamykania systemów operacyjnych poprzez sieć logiczną: Windows Server 2012 Micorosft Hyper-V 2012 Windows Server 2008 Micorosft Hyper-V 2012 Windows Server 2003 Windows 8 WMware ESXi VMware ESX Red Hat Enterprise Linux Ubuntu Linux SuSE Linux Enterprise Server | |
|  | Akcesoria | Szyny montażowe do szafy rack | |
|  | Gwarancja | 1 lata | |

1. **Firewall UTM (dla Gops) szt. 1**

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymagania minimalne** | **Parametry oferowane**  **(w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)** |
| **Ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |  |
| **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. |  |
| **Interfejsy, Dysk, Zasilanie:** | 1. System realizujący funkcję Firewall musi dysponować minimum 4 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC. |  |
| **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 600 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 4,4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,0 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 310 Mbps. |  |
| **Funkcje Systemu Bezpieczeństwa** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy 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. |  |
| **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware vCenter (ESXi). |  |
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/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.  1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:   * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. |  |
| **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. |  |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  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 **3 lat** |  |
| **Gwarancja oraz wsparcie** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |

**6. Firewall UTM (dla Gminy) szt. 1**

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymagania minimalne** | **Parametry oferowane**  **(w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)** |
| **Ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |  |
| **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. |  |
| **Interfejsy, Dysk, Zasilanie:** | 1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC. |  |
| **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 600 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,0 Gbps. 6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 310 Mbps. |  |
| **Funkcje Systemu Bezpieczeństwa** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy 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. |  |
| **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware vCenter (ESXi). |  |
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/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.  1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:   * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. |  |
| **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. |  |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  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 3 **lat** |  |
| **Gwarancja oraz wsparcie** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |

1. **Parametry komputera stacjonarnego (opis)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** | **Parametry oferowane**  **(w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)** |
| 1. | Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja graficzna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu. |  |
| 2. | Obudowa | Typu mini / midi tower z obsługą kart PCI Express.  Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. na napęd optyczny (dopuszcza się stosowanie napedów slim) zewnętrzna, 1 szt. 3,5”na standardowy dysk twardy.  Wyposażona w czytnik kart multimedialnych  Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym  Wyposażona w budowany głośnik o mocy min. 2W lub głośniki w monitorze |  |
| 3. | Zasilacz | Zasilacz minimalnie 500W o sprawności minimum 85% |  |
| 4. | Chipset | Dostosowany do zaoferowanego procesora |  |
| 5. | Płyta główna | Wyposażona w złącza min.:   1. 1 x PCI Express 3.0 x16, 2. 1 x PCI Express 3.0 x1, 3. 1 x M.2 |  |
| 6. | Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi AMD Ryzen 5 5600G na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. |  |
| 7. | Pamięć operacyjna | Min. 16GB DDR4 3200MHz z możliwością rozszerzenia do 32 GB |  |
| 8. | Dysk twardy | Min 256GB SSD M.2 PCIe NVMe zawierający recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |  |
| 9. | Napęd optyczny | Nagrywarka DVD +/-RW |  |
| 10. | Karta graficzna | dedykowana karta graficzna wyposażona w minimum 6 GB RAM, Szyna danych 192 bit  Taktowanie pamięci minimum 15000 MHz, taktowanie rdzenia minimum 1777 Rodzaj pamięci RAM GDDR6 |  |
| 11. | Audio | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. |  |
| 12. | Karta sieciowa | LAN 10/100/1000 Mbit/s z funkją PXE oraz Wake on LAN  WiFi 802.11ac 1x1 + BT 5.0 |  |
| 13. | Porty/złącza | Wbudowane porty/złącza:   1. 1 x VGA, 2. 1 x HDMI, 3. 8 x USB w tym min. 4 x USB3.1 4. port sieciowy RJ-45, 5. porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy 6. czytnik kart pamięci min. SD   Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |  |
| 14. | Monitor | Matryca 23,8” z podświetleniem w technologii LED, Kąt widzenia (stopnie): 178 (pion), 178 (poziom)Czas reakcji: 4 ms Kontrast: 3000:1 |  |
| 15. | Klawiatura/mysz | Klawiatura przewodowa w układzie US  Mysz przewodowa (scroll) |  |
| 16. | System operacyjny | Microsoft Windows 10 64 bit lub Windows 11 64 bit lub równoważny system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 5. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 8. 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, 9. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 10. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 11. Wbudowany system pomocy w języku polskim. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 13. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 14. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 16. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 17. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 18. 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. 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. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 26. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 27. 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.). 28. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 29. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 30. Możliwość tworzenia wirtualnych kart inteligentnych. 31. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (SecureBoot) 32. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 33. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 34. Mechanizmy logowania w oparciu o: 35. Login i hasło, 36. Karty inteligentne i certyfikaty (smartcard), 37. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 38. Certyfikat/Klucz i PIN 39. Certyfikat/Klucz i uwierzytelnienie biometryczne 40. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 41. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 42. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 43. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 44. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń   Nie dopuszcza się zaoferowania systemu operacyjnego typu refurbished. |  |
| 17. | Bezpieczeństwo i zdalne zarządzanie | 1. Czujnik otwarcia obudowy |  |
| 18. | Gwarancja | *2 lata* |  |

1. Oferujemy **okres gwarancji na serwery ………………… miesiące/y.**
2. Oświadczamy, że akceptujemy warunki płatności określone w Specyfikacji Warunkach Zamówienia.
3. Oświadczamy, że jesteśmy związani ofertą od dnia upływu terminu składania ofert do dnia określonego w SWZ.
4. Oświadczamy, że w cenie zostały uwzględnione wszystkie koszty wykonania zamówienia.
5. Oświadczamy, że zapoznaliśmy się z projektowanymi postanowieniami umowy   
   i zobowiązujemy się w przypadku wyboru niniejszej oferty do zawarcia umowy na warunkach w nich określonych.
6. Oświadczamy, że przedmiot zamówienia wykonamy **samodzielnie\*/przy pomocy podwykonawców\***

…………………………………………………………………………………………….……………………………………………………

*(należy wskazać część zamówienia, której wykonanie zamierza powierzyć podwykonawcom oraz podać nazwy podwykonawców jeżeli są już znani).*

1. Oświadczamy, iż wybór naszej oferty **prowadzi\* / nie prowadzi\*** do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą o podatku towarów i usług (art. 225 ustawy Pzp).

…………………………………………………………………………………………………………………………………………………

*(w przypadku, gdy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego należy wskazać nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, wskazać ich wartość towaru lub usługi bez kwoty podatku oraz wskazać stawkę podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie – dla każdej wybranej części zamówienia osobno).*

1. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*\*

*1)rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).*

1. Rodzaj Wykonawcy *(należy wybrać właściwe)*:

mikroprzedsiębiorstwo

małe przedsiębiorstwo

średnie przedsiębiorstwo

prowadzenie jednoosobowej działalności

osoba fizyczna nie prowadząca działalności gospodarczej

inny rodzaj

*Por. zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36). Te informacje są wymagane wyłącznie do celów statystycznych.*

*Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.*

*Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.*

*Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwamii które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EUR.*

……………………………………

*miejscowość, data*

*(należy opatrzyć kwalifikowanym podpisem elektronicznym lub*

*podpisem zaufanym lub podpisem osobistym osoby uprawnionej*

*lub osób uprawnionych do reprezentowania Wykonawcy)*

*\*niewłaściwe skreślić*

*\*\* w przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).*

**UWAGA!**

Wykonawcy składający ofertę wspólnie w miejscu „Pieczęć firmowa Wykonawcy” wpisują dane wszystkich Wykonawców występujących wspólnie.

***Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.***

***Zamawiający zaleca zapisanie dokumentu w formacie PDF.***

*Wzór - załącznik nr 3 do SWZ*

*(obowiązkowy)*

Zamawiający:

**Gmina Szczytno**

**ul. Łomżyńska 3**

**12-100 Szczytno**

**Wykonawca/podmiot udostępniający zasoby/podwykonawca\*:**

……………………………………………

………………………………..................

……………………………………………

*(pełna nazwa/firma, adres,* *w zależności od podmiotu: NIP/KRS)*

**reprezentowany przez:**

……………………………………………

……………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**Oświadczenie Wykonawcy/podmiotu udostępniającego zasoby/podwykonawcy\***

**składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.**

**Prawo zamówień publicznych (dalej jako: Ustawą),**

**DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”** prowadzonego przez **Gminę Szczytno***,* oświadczam, co następuje

**OŚWIADCZENIA DOTYCZĄCE WYKONAWCY / PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY / PODWYKONAWCY1:**

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 Ustawy pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ust. 1 pkt 1,
3. i 7 Ustawy pzp.

3. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

…………….……................................. *(miejscowość),* dnia ………….……..... r.

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …………................ Ustawy pzp*(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 i 6 lub art. 109 ust. 1 pkt 1, 4 i 7 Ustawy pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 Ustawy podjąłem następujące środki naprawcze:

…………………………………………………………………………………...........................................

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………….…..............................…. *(miejscowość),* dnia …………………......... r.

\*– niepotrzebne skreślić;

***Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.***

*Wzór - Załącznik nr 4 do SWZ*

*(obowiązkowy)*

**Zamawiający:**

**Gmina Szczytno**

**ul. Łomżyńska 3**

**12-100 Szczytno**

**Wykonawca/podmiot udostępniający zasoby \*:**

……………………………………………

………………………………..................

……………………………………………

*(pełna nazwa/firma, adres,*

*w zależności od podmiotu: NIP/KRS)*

**reprezentowany przez:**

……………………………………………

……………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**Oświadczenie Wykonawcy/podmiotu udostępniającego zasoby\***

**składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.**

**Prawo zamówień publicznych (dalej jako: Ustawa),**

**DOTYCZĄCE SPEŁNIANIA WARUNKU UDZIAŁU W POSTĘPOWANIU**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”** prowadzonego przez **Gminę Szczytno***,* oświadczam, co następuje:

**INFORMACJA DOTYCZĄCA WYKONAWCY/PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY\*\*:**

Oświadczam, że spełniam warunek udziału w postępowaniu określony przez Zamawiającego w ……………………..…………………………………………………..…………………………………………………………………………………………………………………………………………………………………………………………………………………………….………

*(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu)*.

…………….……. *(miejscowość),* dnia ………….……. r.

**INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW\*\***:

Oświadczam, że w celu wykazania spełniania warunku udziału w postępowaniu, określonego przez Zamawiającego w ………………………………………………………...……….. *(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu),* polegam na zasobach następującego/ych podmiotu/ów:

..…………………….………………………………………………………………………………………………………………………….

w następującym zakresie: …………………………………………..………………………………………………………………...………………………………………

……………………………………………………………………………………………………………………………………………………

*(określić odpowiedni zakres dla wskazanego podmiotu).*

…………….……. *(miejscowość),* dnia ………….……. r.

**\* – niepotrzebne skreślić;**

**\*\*– wypełnia tylko Wykonawca, który w celu wykazania spełnienia warunków udziału polega na zasobach podmiotu**

***Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.***

*Wzór - Załącznik nr 5 do SWZ*

*(obowiązkowy- jeśli dotyczy)*

**Zobowiązanie podmiotu o oddaniu Wykonawcy swoich zasobów**

**w zakresie zdolności technicznych/zawodowych**

Ja/My

.................................................................................................................................................................\*

*(nazwa podmiotu udostępniającego zasoby)*

zobowiązujemy się do oddania do dyspozycji Wykonawcy:

................................................................................................................................................................\*

*(nazwa Wykonawcy ubiegającego się o udzielenie zamówienia)*

niezbędnych zasobów na potrzeby wykonania zamówienia pn. **Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”** w związku z powołaniem się na te zasoby w celu spełniania warunku udziału w postępowaniu przez Wykonawcę w zakresie zdolności technicznych/zawodowych poprzez udział w realizacji zamówienia w charakterze **Podwykonawcy/w innych charakterze\*\*** w zakresie ………………………………………………….\**(należy wypełnić w takim zakresie w jakim podmiot zobowiązuje się oddać Wykonawcy swoje zasoby w zakresie zdolności technicznych/zawodowych)* na okres ……………………………………………………………….……….\*

**\*– należy wypełnić**

**\*\*– niepotrzebne skreślić**

***Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.***

*Wzór - Załącznik nr 6 do SWZ*

*(na wezwanie Zamawiającego)*

**WYKAZ DOSTAW**

Dotyczy: postępowania pn. **Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot realizowanych dostaw** | **Wartość zrealizowanych dostaw (brutto)** | **Czas realizacji dostaw** | **Nazwa podmiotu, na którego rzecz dokonano dostaw** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |

**Do Wykazu załączam dowody potwierdzające, że wskazane dostawy wykonane zostały w sposób należyty.**

***Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.***