Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Znak sprawy: A.ZO.1.23 Horyniec-Zdrój, 28.04.2023 r.

Wójt Gminy Horyniec-Zdrój

zaprasza do składania ofert

do niniejszego zapytania ofertowego związanego z realizacją w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa V „Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU", Działanie 5.1 „Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia", projektu grantowego **„Cyfrowa Gmina"** o numerze POPC.05.01.00-00-0001/21-00, zgodnie z Umową o powierzenie grantu numer 4887/3/2022 prowadzonego przez Gminę Horyniec-Zdrój pod nazwą:

„Dostawa sprzętu komputerowego w ramach projektu grantowego „Cyfrowa Gmina" realizowanego w ramach POPC 2014-2020"

I. Informacje o Zamawiającym:

1. Gminą Horyniec-Zdrój, ul. Aleja Przyjaźni 5, 37-620 Horyniec-Zdrój, NIP 793-15-06-484
2. Osoba upoważniona do kontaktów:

- Piotr Wojtyszyn, komunikacja z Zamawiającym za pośrednictwem portalu Baza Konkurencyjności lub email: sekretarz@horyniec-zdroj.pl
- Mateusz Hejnowicz, email: mateusz@horyniec-zdroj.pl

II. Tryb udzielania zamówienia

Postępowanie prowadzone w oparciu o „Wytyczne w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020", zgodnie z „Zasadą konkurencyjności".

III. Opis przedmiot zamówienia

1. Przedmiotem zamówienia jest dostawa do Urzędu Gminy Horyniec-Zdrój, ul. Aleja Przyjaźni 5, 37-620 Horyniec-Zdrój, NIP 793-15-06-484:

Zadanie zostało podzielone na 2 części :

CZĘŚĆ I

A) Komputer All-in-One – 9 sztuk
B) Urządzenie UTM – 1 sztuka
C) Serwer plików NAS – 1 sztuka

D) Switch – 1 sztuki
E) Zasilanie awaryjne- UPS – 1 sztuk
F) Pakiet oprogramowanie biurowego – 9 sztuk

CZĘŚĆ II

A) Oprogramowania serwera bazy danych – licencja- 30 użytkowników

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Zamawiający wymaga aby zaoferowany sprzęt/oprogramowanie posiadał parametry nie gorsze niż:

CZĘŚĆ I

A)

Komputer stacjonarny typu All-In-One **– 9 sztuki** **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE**		
Szczegółowy opis		
Komputer stacjonarny typu all in one. 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 zaoferowania komputera odnawianego.		
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**
1.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach min. 21 600 pkt. w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/ . Testy pochodzące z okresu od publikacji postępowania do dnia składania ofert. Wydruk z wynikami testów należy załączyć do oferty.
2.	Pamięć operacyjna RAM	Min. 16 GB 4800MHz non-ECC
3.	Parametry pamięci masowej	M.2 512 GB SSD PCIe 4.0 NVMe Możliwość montażu dodatkowego dysku 2,5” SSD lub HDD

4.	Karta graficzna	Zintegrowana z procesorem komputera o wydajności min. 2 600 punktów w teście Average G3D Mark. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. Wynik testu musi pochodzić z okresu od publikacji postępowania do terminu jego składania.
5.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo (2x3W) Port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO) Kamera video z mechaniczną zasłoną obiektywu o rozdzielczości min. 5 MPix i wsparciem dla Windows Hello Dwa mikrofony wbudowane w obudowę komputera
6.	Obudowa	- Zintegrowana z monitorem (AIO) - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, part numberem, numerem seryjnym - Możliwość podpięcia linki zabezpieczającej przez zintegrowane z obudową złącze np. Kensington Lock, Noble Lock
7.	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.
8.	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).
9.	Bezpieczeństwo	TPM 2.0
10.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).

11.	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. 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 wraz z datą produkcji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM - typie procesora i jego prędkości - MAC adresu zintegrowanej karty sieciowej - nr seryjnym płyty głównej komputera - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS - Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Funkcja bezpiecznego usuwania danych z dysku
12.	Ekran	Matowy, matryca IPS lub WVA, 23,8” z podświetleniem w technologii LED Rozdzielczość FHD 1920x1080, Jasność min. 250nits, kontrast 1000:1 Podstawa komputera umożliwiająca regulację wysokości (do 100mm) i pochylenia
13.	Interfejsy / Komunikacja	Wyposażony w minimum: 3x USB typ C w tym min. 2 USB w standardzie 3.x 3x USB typ A w tym min. 2 USB w standardzie 3.x 1x RJ-45 1x HDMI out w standardzie min. 2.0 1x HDMI in w standardzie min. 1.4

		1x port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO)
14.	Karta sieciowa LAN	RJ-45 - 100/1000
15.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX 2x2 Bluetooth 5.1
16.	Klawiatura i mysz	Klawiatura bezprzewodowa w układzie US. Mysz bezprzewodowa z rolką (scroll) Klawiatura i mysz działające na jednym adapterze lub za pomocą połączenia bluetooth.
17.	Zasilacz	Energooszczędny zasilacz o sprawności min. 85 % i mocy nie mniejszej niż 150W
18.	Certyfikaty, oświadczenia i standardy	ENERGY STAR min. 8.0 EPEAT na poziomie min. Silver Deklaracja zgodności CE Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki Certyfikat ISO 9001 dla producenta komputera Certyfikat ISO 14001 dla producenta komputera Certyfikat ISO 50001 dla producenta komputera
19.	Waga/Wymiary	Waga urządzenia z podstawą nie może przekraczać 8 kg.
20.	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
21.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników. 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.
22.	Gwarancja	Minimalny czas trwania gwarancji producenta wynosi 3 lata, świadczona w miejscu użytkowania sprzętu (on-site). Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. W przypadku niewywiązywania się z obowiązku serwisowego przez Autoryzowanego Partnera Serwisowego lub Wykonawcę producent przejmie na siebie obowiązek serwisowy. Komputery musza pochodzić z polskiej dystrybucji producenta. Zamawiający może wystąpić do wykonawców o oświadczenie producenta komputera, potwierdzające spełnienie ww. warunków.
23.	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 Wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera serwisowego dla urządzeń i preinstalowanego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie. 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.

B)

Urządzenie UTM – 1 sztuka
WYMAGANE MINIMALNE PARAMETRY TECHNICZNE

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.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 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 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
5. 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 1.4 Gbps.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 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 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

Polityki, Firewall

13. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. 3. 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.
15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure
    - Google Cloud Platform (GCP).

- OpenStack.
- VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów

oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

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 24 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 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.

Rozszerzone wsparcie serwisowe AHB/SOS

System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.

- 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.

System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

- Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
- Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
- Konfiguracja startowa urządzenia wg ustaleń z zamawiającym.
- Doradztwo w zakresie konfiguracji.
- Zdalne wsparcie techniczne.
- Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
- Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
- Przygotowanie urządzenia do zdalnej konfiguracji.
- Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami

użytkownika.

- Minimum 5 zdalnych rekonfiguracj systemu w związku ze zmianą środowiska lub wymagań użytkownika.
- Minimum dwa razy w roku zdalny przegląd konfiguracji i logów systemu wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

C)

Serwer plików NAS – 1 sztuka
WYMAGANE MINIMALNE PARAMETRY TECHNICZNE

Procesor	Czterordzeniowy o taktowaniu co najmniej 2,2 GHz
Obudowa	Desktop o wymiarach (Wys. x Szer. x Gł.) : 166 X 343 X 243mm
Pamięć RAM	8 GB DDR4 ECC (z możliwością rozbudowy do 32GB)
Ilość obsługiwanych dysków	8 kieszeni na dyski 3,5" lub 2,5" SATA HDD/SSD 2 kieszenie na dyski M.2 2280 NVMe SSD
Interfejsy sieciowe	4 x 1GbE RJ-45
Porty	4 porty USB 3.2 1 gen. 2 porty eSATA
Wskaźniki LED	Status, Alert, LAN, HDD1 - 8
Obsługa RAID	SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych, Sprzętowy moduł szyfrujący
System Operacyjny	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Licencja na Kamery IP	Surveillance Station Maksymalna liczba kamer IP: 40, maks. 1 200 kl./s (FPS) przy rozdzielczości 720p (H.264). (W zestawie dwie licencje)

Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)
Usługi	Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Time Backup, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS, Zarządzanie przez komórkę, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, Możliwość utworzenia klastru HA, Obsługa klastru High Availability
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,
Język GUI	Polski
Gwarancja i serwis	36 miesięcy gwarancji producenta
Waga	Maks. 6 KG
Pobór mocy	Praca maks. 60W / Hibernacja dysków maks. 27W
System plików	Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT
Liczba wolumenów	Do 64
Liczba iSCSI Targetów	Do 128
Liczba iSCSI LUN	Do 256
Liczba kont użytkowników	2048
Liczba grup	256
Liczba udziałów	512
Ilość jednoczesnych połączeń	1000 dla SMB,NFS,AFP,FTP (2000 z rozbudową pamięci RAM)
Głośność	Maks. 23 dB (A)
Chłodzenie	2 wentylatory (120 × 120 mm)
Dyski	4 dyski 4TB SATA, min. 5400RPM, 256MB cache, 1,000,000 MTBF, gwarancja producenta 3 lata, zgodnych z listą kompatybilną podaną przez producenta NAS

D)

Switch- 1 sztuka **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE**

Przełącznik sieciowy

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 60 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.
e) 4 porty 10 GE SFP+.

Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.

- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Centralne zarządzanie konfiguracją urządzenia
   - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   - Centralne zarządzanie sieciami VLAN.
   - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
   - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
   - Automatyczna detekcja i rekomendacje konfiguracji.
   - Przesyłanie logów na zewnętrzny serwer syslog.
   - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   - Obsługa białych i czarnych list adresów MAC.
   - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 24 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.

2. Wsparcie telefoniczne.
   - Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
   - Konfiguracja urządzenia wg ustaleń z zamawiającym.
   - Doradztwo w zakresie konfiguracji.
   - Zdalne wsparcie techniczne.
   - Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
   - Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
   - Przygotowanie urządzenia do zdalnej konfiguracji.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

E)

Zasilanie awaryjne- UPS – 1 sztuka **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE**

UPS 3000W (parametry minimalne)	
Parametr	**Wymagania minimalne**
Moc pozorna	minimum 3000VA
Moc rzeczywista	minimum 3000W
Technologia	on-line (VFI), podwójna konwersja
Sprawność max (dla VFI)	> 90 %
Typ obudowy	rack/tower
Ilość wydzielanego ciepła dla nominalnych warunków pracy	< 1200 BTU / h
praca sieciowa	
Napięcie wejściowe	110 ÷ 300 V AC ± 5%
Częstotliwość napięcia wejściowego	50 / 60 Hz
Zakres napięcia wyjściowego	208 V AC / 220 V AC / 230 V AC / 240 V AC

	± 1 %
Wartość napięcia wyjściowego ustawiana z panelu LCD	tak
Kształt napięcia wyjściowego	sinusoidalny
Czas przełączania sieć – UPS	0ms
Współczynnik odkształceń prądu wejściowego THDi	< 10%
praca bateryjna	
Napięcie wyjściowe	~230V
Częstotliwość napięcia wyjściowego	50Hz/60Hz ± 0,5Hz
Kształt napięcia wyjściowego na pracy bateryjnej	sinusoidalny
Zabezpieczenie przeciwzwarciowe gniazd wyjściowych	Bezpiecznik automatyczny 16 A
Zabezpieczenie przeciążeniowe	elektroniczne
Akumulatory wewnętrzne w UPS / w Module Bateryjnym	minimum 12V 9Ah; szczelne, bezobsługowe
Czas podtrzymania (100 % Pmax) – przy zastosowaniu baterii wewnętrznych lub z zewętrznym modułem bateryjnym.	Minimum 13 minut
pozostałe	
Przeciążalność	110 % ÷ 120 % = 60s, >120 % = 100ms
Wejście zasilania	1 x IEC 320 C20 (16 A)
Typ i ilość gniazd wyjściowych	min 8x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16 A), z czego minimum 4 gniazda sterowalne
Sygnalizacja	Wyświetlacz LCD
Test baterii	wymagana możliwość uruchomienia testu baterii przyciskiem na obudowie zasilacza
Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych	Wymagana możliwość podłączenia do 10 zewnętrznych modułów bateryjnych
Możliwość pracy w trybie konwertera częstotliwości	wymagane
Interfejs komunikacyjny	RS232, USB HID
Możliwość zainstalowania karty SNMP	wymagane
Przewody	min 1szt USB + 2szt IEC 320 C13-C14 10A + 1szt IEC 320 C19-C20 16A
Remote ON/OFF – możliwość zdalnego załączenia/wyłączenia zasilacza	wymagane
Złącze EPO	wymagane ustawienie NC
Waga UPS	do 30kg
Waga MODUŁU BATERYJNEGO – jeżeli występuje	do 42kg
Wymiary UPS – wersja TOWER	nie większe niż: wysokość 439mm; szerokość 88mm; głębokość 611mm
Wymiary MODUŁ BATERYJNY – wersja TOWER, jeżeli występuje	nie większe niż: wysokość 439mm; szerokość 88mm; głębokość 611mm
Gwarancja	minimum 24 miesiące na elektronikę i 24 miesiące na akumulatory;
Serwis	autoryzowany serwis producenta zlokalizowany na terenie Polski
	naprawa w czasie nie dłuższym niż 5 dni roboczych
	serwis realizowany w systemie door to door

Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji Vmware, Hyper-V, Citrix XenServer
	możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPSów
	możliwość zarządzania różnymi UPSami tego samego producenta
	wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
Certyfikaty producenta (załączyć do oferty)	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania;
	deklaracja CE producenta sprzętu
Oświadczenia / dokumenty	oświadczenie producenta o spełnieniu inimalnych wymaganych parametrów specyfikacji
	karta katalogowa oferowanego sprzętu

F)

Pakiet programowania biurowego – 9 szt. WYMAGANE MINIMALNE PARAMETRY TECHNICZNE

Oprogramowanie biurowe	Zintegrowany pakiet aplikacji biurowych pochodzących od jednego producenta, w którego skład ma wchodzić min.: - edytor tekstów; - arkusz kalkulacyjny; - narzędzie do przygotowania i prowadzenia prezentacji; - narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami); - pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. - powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. - dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego - publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu.

	- możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0). Edytor tekstów musi umożliwiać: - Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. - Wstawianie oraz formatowanie tabel. - Wstawianie oraz formatowanie obiektów graficznych. - Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). - Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. - Automatyczne tworzenie spisów treści. - Formatowanie nagłówków i stopek stron. - Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. - Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. - Określenie układu strony (pionowa/pozioma). - Wydruk dokumentów. - Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Arkusz kalkulacyjny musi umożliwiać: - Tworzenie raportów tabelarycznych – - Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych – - Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. - Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice) - Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. - Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych – - Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych - Wyszukiwanie i zamianę danych - Wykonywanie analiz danych przy użyciu formatowania warunkowego - Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie - Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności - Formatowanie czasu, daty i wartości finansowych z polskim formatem - Zapis wielu arkuszy kalkulacyjnych w jednym pliku. - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

	- Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego - Drukowanie w formacie umożliwiającym robienie notatek – - Zapisanie jako prezentacja tylko do odczytu. - Nagrywanie narracji i dołączanie jej do prezentacji - Opatrywanie slajdów notatkami dla prezentera - Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo - Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego - Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym - Możliwość tworzenia animacji obiektów i całych slajdów - Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: - Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, - - Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, - - Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, - Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, - - Automatyczne grupowanie poczty o tym samym tytule, - Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, - Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, - Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, - Zarządzanie kalendarzem, - - Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, - Przeglądanie kalendarza innych użytkowników, - Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, - Zarządzanie listą zadań, - Zlecanie zadań innym użytkownikom, - - Zarządzanie listą kontaktów, - - Udostępnianie listy kontaktów innym użytkownikom, - Przeglądanie listy kontaktów innych użytkowników, - Możliwość przesyłania kontaktów innym użytkowników.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Zamawiający wymaga aby zaoferowany sprzęt/oprogramowanie posiadał parametry nie gorsze niż:

CZĘŚĆ II

A) Oprogramowania serwera bazy danych - 1szt. (dla 30 użytkowników)

Oprogramowania serwera bazy danych - **1 sztuka** **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE**

Przedmiotem zamówienia jest dostawa oprogramowania Microsoft SQL Server 2022 w wersji najnowszej lub oprogramowania równoważnego.

Zakup licencji bezterminowej na system bazodanowy i 30 licencji dla użytkowników systemu bazodanowego. System ten musi obsługiwać minimum 8 rdzeni oraz 64 GB pamięci RAM. Licencja powinna umożliwiać wykorzystywanie systemu na maszynie fizycznej lub wirtualnej.

Dostarczone przedmioty zamówienia muszą być fabrycznie nowe, wolne od wad, a sprzęt zapakowany w opakowania umożliwiające jednoznaczną identyfikację produktu.

Opis kryteriów równoważnych dla oprogramowania.

Jeżeli Zamawiający określił w SOPZ wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający umożliwia dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w SOPZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w SOPZ, w szczególności w zakresie:

a) warunków licencji/sublicencji w każdym aspekcie licencjonowania/ sublicencjonowania
b) funkcjonalności równoważnej oprogramowania
c) oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Microsoft Windows 10 Professional funkcjonującym u Zamawiającego,
d) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego
e) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie.
f) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego

2. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.

3.Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.

4. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w Jego nowszych wersjach.

Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego

1. <u>Funkcjonalność oprogramowania równoważnego do systemu operacyjnego Windows 10 Pro / Windows 11 Pro</u>

1. Interfejs graficzny użytkownika pozwalający na obsługę:
a. Klasyczną przy pomocy klawiatury i myszy.
b. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym polskim i angielskim.
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe.
4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje.
5. Wbudowany system pomocy w języku polskim.
6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.
7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
9. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne.
10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
11. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
12. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.

13. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
15. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
16. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
17. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
18. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.
19. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
20. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
21. Zintegrowany z równoważnym systemem operacyjnym 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.
22. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
23. Obsługa standardu NFC (near field communication).
24. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
25. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
26. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
27. Mechanizmy uwierzytelniania w oparciu o:
a. Login i hasło.
b. Karty z certyfikatami (smartcard).
c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
d. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.
28. Mechanizmy wieloskładnikowego uwierzytelniania.
29. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.
30. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.
31. Wsparcie dla algorytmów Suite B (RFC 4869).
32. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji.
33. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku.
34. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym.
35. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny.

36. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0.
37. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji.
38. Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu.
39. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.
40. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
41. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
42. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.
43. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
44. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego (provisioning).
45. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
46. Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
47. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
48. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
49. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
50. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
51. 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.).
52. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
53. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.
54. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.
55. Wbudowane w równoważnym systemie operacyjnym narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
56. Wbudowane w równoważny system operacyjny narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
57. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
58. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
59. Mechanizm instalacji i uruchamiania równoważnego systemu operacyjnego z pamięci zewnętrznej (USB).
60. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów

wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
61. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
62. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
63. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC.
64. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
65. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
66. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów.
67. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M.
68. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
69. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia.
70. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache”.
71. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji.
72. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością.
73. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji.
74. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
75. Funkcjonalność umożliwiająca na zaktualizowanie systemu bez potrzeby aktualizacji lub przebudowywania paczek aplikacji.
76. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
77. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
78. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym.
79. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
80. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet.
81. Funkcjonalność synchronizacji ustawień aplikacji pomiędzy wieloma komputerami.

2. Jeśli w opisie Przedmiotu Zamówienia występują: nazwy konkretnego producenta, nazwy konkretnego produktu, należy to traktować jako pomoc w opisie Przedmiotu Zamówienia. W każdym przypadku dopuszczalne są produkty posiadające co najmniej takie same lub lepsze parametry techniczne, funkcjonalne i które nie obniżają określonych standardów Przedmiotu Zamówienia. Jeśli w opisie Przedmiotu Zamówienia wskazano jakikolwiek znak towarowy, patent czy pochodzenie – należy przyjąć, że wskazane patenty, znaki towarowe, pochodzenie określają parametry techniczne, eksploatacyjne, użytkowe, co oznacza, że Zamawiający dopuszcza złożenie ofert w tej części Przedmiotu Zamówienia o równoważnych parametrach technicznych i użytkowych. To samo dotyczy sytuacji, gdy Przedmiot Zamówienia opisany jest za pomocą norm, aprobat, specyfikacji technicznych i systemów odniesienia Zamawiający dopuszcza rozwiązania równoważne z opisami.

Główny Kod CPV:

30200000-1 - Urządzenia komputerowe

Pozostałe kody CPV

30236000-2 Różny sprzęt komputerowy

48000000-8 Pakiety oprogramowania i systemy informatyczne

IV. Warunki udziału w postępowaniu

O udzielenie Zamówienia mogą ubiegać się Wykonawcy, którzy spełniają następujące wymagania:

a) posiadają odpowiednie uprawnienia do wykonywania działalności,

Zamawiający nie precyzuje specjalnego warunku w tym zakresie. Ocena spełnienia warunku udziału w postępowaniu dokonywana będzie w oparciu o złożone przez Wykonawcę oświadczenie będące załącznikiem nr 2 do niniejszego Zapytania Ofertowego, według formuły spełnienia – niespełnienia.

b) posiadają wiedzę i doświadczenie,

Zamawiający nie precyzuje specjalnego warunku w tym zakresie. Ocena spełnienia warunku udziału w postępowaniu dokonywana będzie w oparciu o złożone przez Wykonawcę oświadczenie będące załącznikiem nr 2 do niniejszego Zapytania Ofertowego, według formuły spełnienia – niespełnienia.

c) posiadają potencjał techniczny

Zamawiający nie precyzuje specjalnego warunku w tym zakresie. Ocena spełnienia warunku udziału w postępowaniu dokonywana będzie w oparciu o złożone przez Wykonawcę oświadczenie będące załącznikiem nr 2 do niniejszego Zapytania Ofertowego, według formuły spełnienia – niespełnienia.

d) dysponują osobami zdolnymi do wykonania zamówienia

Zamawiający nie precyzuje specjalnego warunku w tym zakresie. Ocena spełnienia warunku udziału w postępowaniu dokonywana będzie w oparciu o złożone przez Wykonawcę oświadczenie będące załącznikiem nr 2 do niniejszego Zapytania Ofertowego, według formuły spełnienia – niespełnienia.

e) posiadają odpowiednią sytuację ekonomiczną i finansową do wykonania zamówienia.

Zamawiający nie precyzuje specjalnego warunku w tym zakresie. Ocena spełnienia warunku udziału w postępowaniu dokonywana będzie w oparciu o złożone przez Wykonawcę oświadczenie będące załącznikiem nr 2 do niniejszego Zapytania Ofertowego, według formuły spełnienia – niespełnienia.

Oferty Wykonawców, którzy nie spełnią warunków udziału w postępowaniu, zostaną odrzucone.

V. Kryteria oceny ofert wraz z informacją o wagach punktowych przypisanych do poszczególnych kryteriów oceny oferty

Kryteria oceny ofert - zamawiający uzna oferty za spełniające wymagania i przyjmie do szczegółowego rozpatrywania, jeżeli:

1. oferta spełnia wymagania określone w niniejszym zapytaniu ofertowym
2. oferta została złożona, w określonym przez Zamawiającego miejscu i terminie,
3. zamawiający zastrzega możliwość weryfikacji parametrów technicznych zaoferowanego sprzętu. Jeśli Zamawiający jednoznacznie stwierdzi, że zaoferowany sprzęt nie spełnia wymogów określonych w zapytaniu Ofertowym, uzna złożoną ofertę za nie spełniającą wymagań Zamawiającego. W przypadku wątpliwości w zakresie parametrów zaoferowanego sprzętu, zamawiający może wystąpić o dodatkowe wyjaśnienia.

Oferty Wykonawców, którzy nie spełnią ww. wymagań zostaną odrzucone.

Zamawiający wyznaczył następujące kryteria oceny i wyboru ofert:

Lp	Nazwa kryterium	Waga kryterium
1.	Cena	100,00 pkt

VI. Opis sposobu przyznawania punktacji za spełnienie danego kryterium oceny ofert

Zastosowane wzory do obliczenia punktowego:

a)Liczba punktów uzyskanych w kryterium **„Cena”** będzie obliczana zgodnie z poniższym wzorem:

$$P = \frac{C_{min}}{C_{bad}} \times 100 \text{ pkt}$$ (zaokrąglone do 2 miejsca po przecinku)

gdzie: C_{min} – najniższa cena brutto spośród badanych ofert
C_{bad} – cena brutto oferty badanej
C – liczba punktów badanej oferty w kryterium najniższa cena

Za najkorzystniejszą uznana zostanie oferta, która uzyska najwyższą liczbę punktów (P).

VII. Termin i miejsce składania ofert oraz sposób złożenia oferty

1. Ofertę należy przesłać **za pośrednictwem portalu Baza Konkurencyjności**

do dnia 12.05.2023 r. do godz. 12.00

Oferty złożone po terminie nie będą rozpatrywane.

2. Zamawiający wymaga, aby oferta zawierała następujące dokumenty:
   1) wypełniony i podpisany przez Wykonawcę formularz cenowo - ofertowy – wg. załączonego wzoru formularza ofertowego –zał nr 1, oryginał
   2) wypełnione i podpisane oświadczenie o spełnieniu warunków udziału w postępowaniu–zał nr 2, oryginał
   3) Wypełnione i podpisane oświadczenie o braku podstaw do wykluczenia z postępowania - zał nr 3, oryginał

3. Oferta powinna być podpisana przez uprawnioną do tego osobę (lub osoby), zgodnie z zasadami reprezentacji danego Wykonawcy. W przypadku ustanowienia pełnomocnictwa, do oferty należy dostarczyć stosowny dokument.

VIII. Termin zakończenia realizacji umowy/zamówienia

Termin realizacji umowy/zamówienia**:** do 30 dni kalendarzowych od dnia podpisania umowy

IX. Informacja na temat zakresu wykluczenia

W postępowaniu nie mogą brać udziału podmioty powiązane osobowo lub kapitałowo z Zamawiającym. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w szczególności na:

1) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
2) posiadaniu udziałów lub co najmniej 10% lub akcji,
3) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
4) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

Ponadto z postępowania o udzielenie zamówienia publicznego wyklucza się, na podstawie art. 7 ust. 9 w związku z 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 (Dz. U. z 2022 r., poz. 835):

Na podstawie art. 7 ust. 1 ww. ustawy wyklucza się:

1) wykonawcę wymienionego w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.), zwanego dalej „rozporządzeniem 765/2006" i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6 z późn. zm.), zwanego dalej „rozporządzeniem 269/2014" albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy,

2) wykonawcę, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2022 r. poz. 593 z późn. zm.) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy,

3) wykonawcę, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. z 2021 r. poz. 217 z późn. zm.) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

Powyższe wykluczenie następować będzie na okres trwania ww. okoliczności.

Zamawiający uzna, że Wykonawca nie podlega wykluczeniu jeżeli złoży oświadczenie o braku podstaw do wykluczenia. Oświadczenie stanowi zał nr 3 do niniejszego zapytania ofertowego. Oferty Wykonawców, którzy nie podpiszą ww. oświadczenia lub go nie złożą z ofertą, zostaną odrzucone.

X. Określenie warunków zmian umowy zawartej w wyniku przeprowadzonego postępowania o udzielenie zamówienia, o ile przewiduje się możliwość zmiany takiej umowy

Zamawiający dopuszcza możliwość zmian postanowień zawartych w umowie w przypadku, gdy wyposażenie przedstawione w ofercie w momencie dostawy:

a) nie będzie dostępne na rynku,
b) będzie wycofane ze sprzedaży przez producenta/dystrybutora
c) producent/dystrybutor wprowadzi nowszy model

przewiduje się dopuszczenie innego wyposażenia pod warunkiem, że parametry techniczne będą spełniały wymagania określone w Zapytaniu ofertowym, a cena nie ulegnie zmianie.

XI. Informacja o możliwości składania ofert częściowych

Zamawiający dopuszcza składanie ofert częściowych. Zamawiający podzielił zamówienie na dwie części.

XII. Opis sposobu przedstawiania ofert wariantowych

Zamawiający nie dopuszcza składania ofert wariantowych.

XIII. Informację o planowanych zamówieniach dodatkowych / uzupełniających

Zamawiający nie przewiduje udzielanie zamówień dodatkowych lub uzupełniających.

XIV. Dodatkowe postanowienia

a) Zapytanie ofertowe zostanie umieszczone na stronie internetowej: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, oraz na stronie internetowej Zamawiającego https://bip.horyniec-zdroj.pl/

b) Złożenie przez Wykonawcę fałszywych lub stwierdzających nieprawdę dokumentów lub nierzetelnych oświadczeń mających istotne znaczenie dla prowadzonego postępowania spowoduje wykluczenie Wykonawcy z dalszego postępowania.

c) Wybór najkorzystniejszej oferty zostanie udokumentowany protokołem postępowania o udzielenie zamówienia publicznego, oraz informacją o wyniku postepowania umieszczoną na

stronie internetowej: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, oraz na stronie internetowej Zamawiającego https://bip.horyniec-zdroj.pl/

d) Niezwłocznie po wyborze najkorzystniejszej oferty, Zamawiający zawiadomi wszystkich Wykonawców, którzy ubiegali się o udzielenie zamówienia o wyniku postępowania.

e) Zamawiający zastrzega możliwość unieważnienia postępowania bez podania przyczyny.

XV. Termin związania ofertą.

1. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. Wykonawca pozostaje związany ofertą przez okres 30 dni.

XVI. RODO

Postępowanie prowadzone jest w celu realizacji projektu grantowego finansowanego w ramach Programu Polska Cyfrowa 2014-2020 (POPC 2014-2020)

Ze względu na to, że to Minister Funduszy i Polityki Regionalnej - jako Instytucja Zarządzająca POPC 2014-2020 - określa: jakie dane osobowe, w jaki sposób i w jakim celu będą przetwarzane w związku z realizacją Programu, pełni on rolę administratora danych osobowych przetwarzanych w związku z realizacją POPC 2014-2020 w rozumieniu RODO [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) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE. L Nr 119, str. 1).]. Przy czym jest on administratorem zarówno wobec danych osobowych, które samodzielnie pozyskał, jak i wobec danych osobowych pozyskanych przez inne podmioty zaangażowane w realizację Programu (tj. przez innych administratorów, którzy w tym przypadku pełnią dodatkowo funkcję podmiotów przetwarzających dane osobowe [Podmiotami przetwarzającymi są: Instytucja Pośrednicząca POPC 2014-2020, beneficjenci oraz inne podmioty zaangażowane w realizację POPC 2014-2020, którym Minister (lub inny upoważniony podmiot) powierzył przetwarzanie danych osobowych w ramach POPC 2014-2020]).

Minister Funduszy i Polityki Regionalnej jest także administratorem danych osobowych, które przetwarza jako beneficjent projektów współfinansowanych ze środków POPC 2014-2020.

Minister Funduszy i Polityki Regionalnej jest również administratorem danych zgromadzonych w zarządzanym przez niego Centralnym Systemie Teleinformatycznym wspierającym realizację POPC 2014-2020.

Cel przetwarzania danych osobowych

Minister Funduszy i Polityki Regionalnej przetwarza dane osobowe w celu realizacji zadań przypisanych Instytucji Zarządzającej POPC 2014-2020, w zakresie w jakim jest to niezbędne dla realizacji tego celu. Minister Funduszy i Polityki Regionalnej przetwarza dane osobowe w szczególności w celach:

1. udzielania wsparcia beneficjentom ubiegającym się o dofinansowanie i realizującym projekty,
2. potwierdzania kwalifikowalności wydatków,
3. wnioskowania o płatności do Komisji Europejskiej,
4. raportowania o nieprawidłowościach,
5. ewaluacji,

6. monitoringu,
7. kontroli,
8. audytu,
9. sprawozdawczości oraz
10. działań informacyjno-promocyjnych.

Podstawy prawne przetwarzania

Przetwarzanie danych osobowych w związku z realizacją POPC 2014-2020 odbywa się zgodnie z RODO.

Podstawą prawną przetwarzania danych jest konieczność realizacji obowiązków spoczywających na Ministrze Funduszy i Polityki Regionalnej - jako na Instytucji Zarządzającej - na podstawie przepisów prawa europejskiego i krajowego (art. 6 ust. 1 lit. c RODO).

Obowiązki te wynikają m.in. z przepisów ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 oraz przepisów prawa europejskiego:

1. rozporządzenia Parlamentu Europejskiego i Rady nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego, oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego Rozporządzenie Rady (WE) nr 1083/2006,
2. rozporządzenia wykonawczego Komisji (UE) nr 1011/2014 z dnia 22 września 2014 r. ustanawiającego szczegółowe przepisy wykonawcze do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 w odniesieniu do wzorów służących do przekazywania Komisji określonych informacji oraz szczegółowe przepisy dotyczące wymiany informacji między beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi. Podstawą przetwarzania danych osobowych przez Ministra są również:

1. konieczność realizacji umowy, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. b RODO) - podstawa ta ma zastosowanie m. in. do danych osobowych osób prowadzących samodzielną działalność gospodarczą, z którymi Minister zawarł umowy w celu realizacji POPC 2014-2020,
2. wykonywanie zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Ministrowi (art. 6 ust. 1 lit e RODO) -podstawa ta ma zastosowanie m. in. do organizowanych przez Ministra konkursów i akcji promocyjnych dotyczących Programu,
3. uzasadniony interes prawny Ministra Funduszy i Polityki Regionalnej (art. 6 ust. 1 lit f RODO) – podstawa ta ma zastosowanie m.in. do danych osobowych przetwarzanych w związku z realizacją umów w ramach Funduszy Europejskich. W ramach POPC 2014-2020 w działaniu 3.1 - Działania szkoleniowe na rzecz rozwoju kompetencji cyfrowych przetwarzane są dane szczególnej kategorii (dane o niepełnosprawności). Podstawą prawną ich przetwarzania jest wyraźna zgoda osoby, której dane dotyczą (art. 9 ust. 2 lit a RODO).

Rodzaje przetwarzanych danych

Minister Funduszy i Polityki Regionalnej w celu realizacji POPC 2014-2020 przetwarza dane osobowe m. in.:

1. pracowników, wolontariuszy, praktykantów i stażystów reprezentujących lub wykonujących zadania na rzecz podmiotów zaangażowanych w obsługę i realizację POPC 2014-2020,
2. osób wskazanych do kontaktu, osób upoważnionych do podejmowania wiążących decyzji oraz innych osób wykonujących zadania na rzecz wnioskodawców, beneficjentów i partnerów,
3. uczestników szkoleń, konkursów, konferencji, komitetów monitorujących, grup roboczych, grup sterujących oraz spotkań informacyjnych lub promocyjnych organizowanych w ramach POPC 2014-2020,
4. kandydatów na ekspertów oraz ekspertów zaangażowanych w proces wyboru projektów do dofinansowania lub wykonujących zadania związane z realizacją praw i obowiązków właściwych instytucji, wynikających z zawartych umów o dofinansowanie projektów,
5. osób, których dane będą przetwarzane w związku z badaniem kwalifikowalności środków w projekcie, w tym w szczególności: personelu projektu, uczestników komisji przetargowych, oferentów i wykonawców zamówień publicznych, osób świadczących usługi na podstawie umów cywilnoprawnych.

Wśród rodzajów danych osobowych przetwarzanych przez Ministra można wymienić:

1. dane identyfikacyjne, w szczególności: imię, nazwisko, miejsce zatrudnienia/formę prowadzenia działalności gospodarczej, stanowisko; w niektórych przypadkach także nr PESEL/NIP/REGON,
2. dane dotyczące stosunku pracy, w szczególności otrzymywane wynagrodzenie oraz wymiar czasu pracy,
3. dane kontaktowe, które obejmują w szczególności adres e-mail, nr telefonu, nr fax, adres do korespondencji,
4. dane o charakterze finansowym, w szczególności nr rachunku bankowego, kwotę przyznanych środków, informacje dotyczące nieruchomości (nr działki, nr księgi wieczystej) kwotę wynagrodzenia,
5. dane zbierane w celu realizacji obowiązków sprawozdawczych do których realizacji zobowiązane są państwa członkowskie, obejmujące w szczególności: płeć, wiek w chwili przystąpienia do projektu, wykształcenie, wykonywany zawód, narodowość, informacje o niepełnosprawności.

Dane pozyskiwane są bezpośrednio od osób, których dane dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację programów operacyjnych, w szczególności wnioskodawców, beneficjentów i partnerów.

W przypadku, gdy dane pozyskiwanie są bezpośrednio od osób, których dane dotyczą, podanie danych jest dobrowolne. Odmowa podania danych jest jednak równoznaczna z brakiem możliwości podjęcia stosownych działań, np. ubiegania się o środki w ramach POPC 2014-2020.

Okres przechowywania danych

Dane osobowe będą przechowywane przez okres wskazany w art. 140 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. oraz jednocześnie przez czas nie krótszy niż 10 lat od dnia przyznania ostatniej pomocy w ramach POPC 2014-2020 - z równoczesnym uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

W niektórych przypadkach, np. prowadzenia kontroli u Ministra przez organy Unii Europejskiej, okres ten może zostać wydłużony.

Odbiorcy danych

Odbiorcami danych osobowych mogą być:

* podmioty, którym Instytucja Zarządzająca POPC 2014-2020 powierzyła wykonywanie zadań związanych z realizacją Programu, w tym w szczególności Instytucja Pośrednicząca POPC, a także eksperci, podmioty prowadzące audyty, kontrole, szkolenia i ewaluacje,

* instytucje, organy i agencje Unii Europejskiej (UE), a także inne podmioty, którym UE powierzyła wykonywanie zadań związanych z wdrażaniem POPC 2014-2020,

* podmioty świadczące na rzecz Ministra usługi związane z obsługą i rozwojem systemów teleinformatycznych oraz zapewnieniem łączności, w szczególności dostawcy rozwiązań IT i operatorzy telekomunikacyjni.

Prawa osoby, której dane dotyczą

Osobom, których dane przetwarzane są w związku z realizacją POPC 2014-2020 przysługują następujące prawa:

1. prawo dostępu do danych osobowych i ich sprostowania.

Realizując te prawo, osoba której dane dotyczą może zwrócić się do Ministra z pytanie m.in. o to czy Minister przetwarza jej dane osobowe, jakie dane osobowe przetwarza i skąd je pozyskał, jaki jest cel przetwarzania i jego podstawa prawna oraz jak długo dane te będą przetwarzane. W przypadku, gdy przetwarzane dane okażą się nieaktualne, osoba, której dane dotyczą może zwrócić się do Ministra z wnioskiem o ich aktualizację;

2. prawo usunięcia lub ograniczenia ich przetwarzania – jeżeli spełnione są przesłanki określone w art. 17 i 18 RODO.

Żądanie usunięcia danych osobowych realizowane jest w szczególności gdy dalsze przetwarzanie danych nie jest już niezbędne do realizacji celu Ministra lub dane osobowe były przetwarzane niezgodnie z prawem. Szczegółowe warunki korzystania z tego prawa określa art. 17 RODO. Ograniczenie przetwarzania danych osobowych powoduje, że Minister może jedynie przechowywać dane osobowe. Minister nie może przekazywać tych danych innym podmiotom, modyfikować ich ani usuwać.

Ograniczanie przetwarzania danych osobowych ma charakter czasowy i trwa do momentu dokonania przez Ministra oceny, czy dane osobowe są prawidłowe, przetwarzane zgodnie z prawem oraz niezbędne do realizacji celu przetwarzania.

Ograniczenie przetwarzania danych osobowych następuje także w przypadku wniesienia sprzeciwu wobec przetwarzania danych – do czasu rozpatrzenia przez Ministra tego sprzeciwu;

3. prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;

4. prawo do cofnięcia zgody, w każdym momencie - w przypadku, gdy podstawą przetwarzania danych jest zgoda (art. 9 ust. 2 lit a RODO). Cofnięcie zgody nie spowoduje, że dotychczasowe przetwarzanie danych zostanie uznane za niezgodne z prawem;

5. prawo otrzymania danych osobowych w ustrukturyzowanym powszechnie używanym formacie, przenoszenia tych danych do innych administratorów lub żądania, o ile jest to technicznie możliwe, przesłania ich przez administratora innemu administratorowi - w przypadku, gdy podstawą

przetwarzania danych jest zgoda lub realizacja umowy z osobą, której dane dotyczą (art. 6 ust. 1 lit b RODO);

6. prawo wniesienia sprzeciwu wobec przetwarzania danych osobowych - w przypadku, gdy podstawą przetwarzania danych jest realizacja zadań publicznych administratora lub jego prawnie uzasadnionych interesów (art. 6 ust. 1 lit e lub f RODO). Wniesienie sprzeciwu powoduje zaprzestanie przetwarzania danych osobowych przez Ministra, chyba że wykaże on, istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Zautomatyzowane podejmowanie decyzji

Dane nie podlegają procesowi zautomatyzowanego podejmowania decyzji.

Kontakt z Inspektorem Ochrony Danych

Ministerstwo Funduszy i Polityki Regionalnej ma swoją siedzibę pod adresem: ul. Wspólna 2/4, 00-926 Warszawa. W przypadku pytań, kontakt z Inspektorem Ochrony Danych MFiPR jest możliwy: pod adresem: ul. Wspólna 2/4, 00-926 Warszawa, pod adresem poczty elektronicznej: IOD@mfipr.gov.pl

Klauzula informacyjna z art. 13 ust. 1 i 2 RODO
w celu związanym z postępowaniem o udzielenie zamówienia publicznego

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia 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), dalej „Rozporządzenie", informuję, że:

1. Administratorem Pani/Pana danych osobowych jest **Urząd Gminy Horyniec- Zdrój reprezentowany przez Wójta Gminy Horyniec- Zdrój** (al. Przyjaźni 5, 37-620 Horyniec- Zdrój; tel. 16 6313455 adres e-miał: ug@horyniec-zdroj.pl)
2. W sprawach z zakresu ochrony danych osobowych może się Pani/Pan kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail: inspektor@cbi24.pl lub pisemnie na adres Administratora.
3. Pani/Pana dane osobowe będą przetwarzane w celu związanym z postępowaniem prowadzonym z wyłączeniem przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019r. poz. 2019 ze zm.).
4. Pani/Pana dane osobowe będą przetwarzane przez okres 5 pełnych lat kalendarzowych, licząc od 1 stycznia roku następnego po roku, w którym nastąpiło zakończenie sprawy (11 lat) na podstawie Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.
5. Podstawą prawną przetwarzania Pani/Pana danych jest art. 6 ust. 1 lit. c) ww. Rozporządzenia w związku z przepisami ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2020 r. poz. 713 z późn. zm.). 6. Pani/Pana dane osobowe będą ujawniane osobom działającym z upoważnienia administratora, mającym dostęp do danych osobowych i przetwarzającym je wyłącznie na polecenie administratora, chyba że wymaga tego prawo UE lub prawo państwa członkowskiego. Pani/Pana dane mogą zostać przekazane podmiotom zewnętrznym na podstawie umowy powierzenia przetwarzania danych

osobowych - dostawcy usług poczty mailowej, strony BIP, dostawcy usług informatycznych w zakresie programów księgowo-ewidencyjnych.
7. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych związanym z udziałem w postępowaniu; konsekwencją niepodania danych jest brak możliwości udziału w postępowaniu.
8. Osoba, której dane dotyczą ma prawo do:
- dostępu do treści swoich danych oraz możliwości ich poprawiania, sprostowania, ograniczenia przetwarzania,
- w przypadku gdy przetwarzanie danych odbywa się z naruszeniem przepisów Rozporządzenia służy prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
9. Osobie, której dane dotyczą nie przysługuje:
- w związku z art. 17 ust. 3 lit. b, d lub e Rozporządzenia prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 Rozporządzenia;
- na podstawie art. 21 Rozporządzenia prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c Rozporządzenia.
10. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego.
11. Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 Rozporządzenia, nie może skutkować zmianą wyniku postępowania ani zmianą postanowień umowy.
12. Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 Rozporządzenia, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania.
14. Od dnia zakończenia postępowania o udzielenie zamówienia, w przypadku gdy wniesienie żądania, o którym mowa w art. 18 ust. 1 Rozporządzenia, spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole i załącznikach do protokołu, Administrator nie udostępnia tych danych zawartych w protokole i w załącznikach do protokołu, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 Rozporządzenia.
15. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających w szczególności na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.
16. Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia, o którym mowa w art. 16 Rozporządzenia, nie może naruszać integralności protokołu oraz jego załączników.
17. Ponadto informujemy, iż w związku z przetwarzaniem Pani/Pana danych osobowych nie podlega Pan/Pani decyzjom, które się opierają wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 Rozporządzenia.

Wójt Gminy Horyniec-Zdrój
/-/ Robert Serkis

Signed by / Podpisano przez:
Robert Marek Serkis
Date / Data: 2023-04-28 11:38

Załączniki:

1. Formularz cenowo – ofertowy
2. Oświadczenie o spełnieniu warunków udziału w postępowaniu
3. Oświadczenie o braku podstaw do wykluczenia z postępowania
4. Projekt umowy