

Lista pozycji budżetowych projektu

SPECYFIKACJA DOSTAW

Tytuł projektu:		"Platforma e-usług publicznych w Mieście Radymno "			
Wnioskodawca:		Miasto Radymno			
Lp.	Nazwa środka trwałego lub wartości niematerialnych i prawnych itp.	Opis głównych parametrów technicznych	Nazwa zadania zgodna z sekcją V wniosku - Budżet projektu	Jednostka miary	Ilość
1	eBOM - elektroniczne Biuro Obsługi Mieszkańca	<p>Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę.</p> <p>1.eBOM (Elektroniczne Biuro Obsługi Mieszkańca) będzie miało za zadanie udostępniać e-usługi świadczone na rzecz mieszkańców Gminy.</p> <p>2.Celem portalu jest zebranie w jednym miejscu informacji obejmującej różne aspekty działalności Urzędu/Gminy. Aby informacja ta była łatwo dostępna, treści publikowane w portalu zostaną podzielone tematyczne. Karty e-usługi powinny być pogrupowane wg. wydziałów wraz z możliwością wyszukiwania ich za pomocą haseł tematycznych. System powinien umożliwić publikowanie danych otwartych w ogólnodostępnej części wg. podziałów na grupy danych z możliwością obsługi różnych formatów danych do pobrania oraz wywoływania adresów serwisów zawierających odpowiednie informacje.</p> <p>3.eBOM zostanie zrealizowany jako serwis WWW dostępny publicznie w sieci Internet z wydzieleniem części ogólnie dostępnej dla użytkowników anonimowych oraz części dostępnej po uwierzytelnieniu użytkownika. Formatowanie publikowanych treści ma następować w oparciu o zdefiniowane szablony, zapewniające spójną prezentację informacji na całej platformie.</p> <p>4.Dostarczane rozwiązanie będzie zgodne z</p>	Platforma e-usług publicznych	lic.	1



		<p>obowiązującym stanem prawnym, przepisami prawnymi regulującymi działalność samorządu we wszystkich dziedzinach jego funkcjonowania. W szczególności należy podkreślić zgodność z Krajowymi Ramami Interoperacyjności. Dostarczony system powinien mieć możliwość obsługi za pomocą najpopularniejszych przeglądarek internetowych a także za pomocą urządzeń mobilnych. EBOM musi się charakteryzować wysoką dostępnością i być zgodny ze standardami dostępności treści internetowych WCAG 2.1. Portal będzie w sposób intuicyjny kierował użytkownikami dając możliwość przechodzenia od ogółu do szczegółu. 5. Portal będzie miał także możliwość integracji z kartami usług platformy ePUAP oraz zapewni możliwość publikowania własnych dokumentów do pobrania, np. w formacie rtf czy pdf. 5. Platforma eBOM w zakresie integracji z innymi serwisami powinna wykorzystywać elementy architektury opartej na usługach (ang. Service-Oriented Architecture, SOA). Powinna udostępniać API na potrzeby wymiany danych.</p>			
2	Aplikacja mobilna	<p>Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę.</p> <ol style="list-style-type: none"> 1. Aplikacja musi zostać zintegrowana z posiadanym przez Wnioskodawcę systemem dziedzinowym oraz posiadaną stroną www. 2. Aplikacja musi zapewniać klucz API do aplikacji zewnętrznych. 3. Aplikacja mobilna powinna być dostępna w wersjach na popularne systemy operacyjne stosowane dla urządzeń mobilnych (Android, iOS) 3. Aplikacja powinna być podzielona na strefę ogólnodostępną oraz strefę użytkownika zalogowanego. 4. Aplikacja powinna zapewniać bezpieczne logowanie przez autoryzację z wykorzystaniem powszechnie dostępnego profilu zaufanego (https://pz.gov.pl) za pośrednictwem krajowego węzła identyfikacji elektronicznej. 	Platforma e-usług publicznych	lic.	1

		<p>5. Zalogowany użytkownik musi posiadać dostęp do danych z systemów dziedzinowych w zakresie wymaganym dla portalu eBOM z możliwością dokonywania zapłat. Wizualizacja danych w swoim zakresie i sposobie prezentowania powinna być w miarę możliwości technicznych jednolita.</p> <p>6. Aplikacja musi umożliwić prezentację załączników (dokumentów z systemów dziedzinowych) z wykorzystaniem formatu PDF.</p> <p>7. Aplikacja mobilna musi otrzymywać powiadomienia z systemów dziedzinowych zgodnie z ustawieniami w ich modułach i kontem zalogowanego użytkownika.</p> <p>8. Powiadomienia będą spersonalizowane i wysyłane do konkretnych użytkowników zarejestrowanych w systemie.</p> <p>9. Zalogowany użytkownik powinien mieć możliwość włączenia lub wyłączenia wybranego typu powiadomienia oraz określenie metody jego dostarczania.</p> <p>10. Aplikacja umożliwi automatyczne wysłanie e-maili do gminy. System umożliwi wybranie tematu wiadomości i automatycznie skieruje ją do osoby odpowiedzialnej za dane zadanie.</p> <p>11. Aplikacja powinna być udostępniona na powszechnie dostępnych serwisach do ich pobierania.</p>			
3	Oprogramowanie dziedzinowe	<p>Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę..</p> <p>1. Pozycja dotyczy podniesienia wersji posiadanego systemu dziedzinowego do najnowszej wspieranej przez producenta wersji.</p> <p>2. Aktualizacja ma dotyczyć wszystkich pozycji wchodzących w skład tzw. aplikacji dziedzinowych – specjalizowane programy przeznaczone do obsługi wydzielonych obszarów aktywności jednostek administracji.</p> <p>3. Przystosowanie systemów dziedzinowych do przekazywania danych do platformy EBOM celem świadczenia e-usług publicznych.</p> <p>4. Przystosowanie oprogramowania do świadczenia</p>	Platforma e-usług publicznych	lic.	1

		<p>płatności elektronicznych.</p> <p>5. Zapewnienie logowania z wykorzystaniem kont domnowych.</p> <p>6. Wprowadzenie wersjonowania.</p> <p>7. Logowania zdarzeń bezpieczeństwa.</p> <p>8. Szyfrowanie danych i komunikacji przesyłu danych.</p> <p>9. Zapewnienie otwartych mechanizmów wymiany danych z aplikacjami zewnętrznymi - interfejs API.</p>			
4	System GIS	<p>Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę.</p> <p>Modernizacja obecnego Systemu Informacji Przestrzennej wraz z integracją z dziedzinowymi Systemami w zakresie obsługi E-usług.</p> <p>1. Pozycja dotyczy podniesienia wersji posiadanego systemu GIS do najnowszej wspieranej przez producenta wersji.</p> <p>2. Aktualizacja ma dotyczyć wszystkich pozycji wchodzących w skład Systemu GIS – specjalizowane programy przeznaczone do obsługi wydzielonych obszarów aktywności jednostek administracji.</p> <p>3. Przystosowanie systemów GIS do przekazywania danych do platformy EBOM celem świadczenia e-usług publicznych.</p> <p>4. Przystosowanie oprogramowania do świadczenia płatności elektronicznych.</p> <p>5. Zapewnienie logowania z wykorzystaniem kont domnowych.</p> <p>6. Wprowadzenie wersjonowania.</p> <p>7. Logowania zdarzeń bezpieczeństwa.</p> <p>8. Szyfrowanie danych i komunikacji przesyłu danych.</p> <p>9. Zapewnienie otwartych mechanizmów wymiany danych z aplikacjami zewnętrznymi - interfejs API.</p> <p>Zakres modułów:</p> <p>a. Planowanie przestrzenne</p> <p>b. Ewidencje</p> <p>c. Środowisko</p> <p>d. Oświetlenie uliczne</p> <p>e. Drogi</p> <p>f. Ewidencja cmentarzy</p>	Platforma e-usług publicznych	lic.	1

		<p>g. Zgłoszenia</p> <p>System GIS (gdzie wszystkie wymagania funkcjonalne Systemu GIS będą realizowane przez aplikację internetową za pośrednictwem przeglądarki internetowej) służy do gromadzenia, przechowywania, analizy i wizualizacji danych przestrzennych. Podstawowym elementem całego zadania będzie digitalizacja danych przestrzennych (z obszaru uchwał oraz rejestrów gminnych) oraz ich migracja do specjalistycznych systemów dziedzinowych Systemu GIS. Pozycja ma na celu usprawnienie pracy Urzędu, publikacji tych danych w wybranych obszarach oraz uruchomieniu E-usług publicznych dla mieszkańców i innych interesariuszy.</p>			
5	eRada	<p>Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę.</p> <p>System do obsługi e-rady, transmisji obrad pozwalający na zdalne uczestniczenie w obradach osobom zainteresowanym. System powinien posiadać następujące funkcjonalności:</p> <p>a) możliwość nagrywania obrad rady oraz ich bieżącej prezentacji w systemach streamingowych lub na ogólnie dostępnych portalach np. youtube, lub na stronie własnej gminy</p> <p>b) system do prowadzenia obrad rady z możliwością przyznawania głosu poszczególnym członkom, osobom zewnętrznym, kolejowania głosu, śledzenia głosowań, itp.</p> <p>c) możliwość udzielania głosu i połączenia głosowego oraz video z zewnętrznymi obserwatorami obrad (mieszkańcami) celem umożliwienia im wypowiedzi/zadania pytań.</p> <p>d) możliwość zarządzania dokumentami dla radnych (publikacja, zapewnienie dostępu do dokumentów w wersji cyfrowej, potwierdzenie otrzymania, itp.)</p> <p>e) integracja z systemem eBOM celem prezentacji treści i umożliwienia dostępu do usługi bezpośrednio z systemu eBOM</p>	Platforma e-usług publicznych	lic.	1

		Wydatek obejmuje podniesienie aktualnie posiadanych funkcjonalności do najwyższych dostępnych wersji. Aktualizacja ma dotyczyć wszystkich funkcjonalności wymienionych powyżej i wchodzących w skład systemu, pozwalających na świadczenie e-usługi w sposób zgodny z wymogami bezpieczeństwa informatycznego urzędu.			
6	Obieg dokumentów	<p>Oprogramowanie - licencja jednostkowa - na osobę/pracownika.</p> <ol style="list-style-type: none"> Oprogramowanie EZD służyć będzie Zamawiającemu do: <ol style="list-style-type: none"> realizacji zadań wynikających z instrukcji kancelaryjnej. wspierania działalności w różnych obszarach biznesowych w tym świadczenia e-usług usprawnienia pracy urzędu. Dostarczony system będzie obsługiwał obieg korespondencji, prowadzenie spraw. EZD będzie możliwy do integracji z innymi systemami dzięki posiadanym interfejsom komunikacyjnym. EZD mieć strukturę modułową, EZD musi pozwalać na wykonywanie kopii bezpieczeństwa, EZD musi zapewniać jednoznaczne przypisanie odpowiedzialności za każdy z dokumentów, EZD musi zapewniać jednoznaczną i niepodważalną identyfikację użytkowników pracujących w systemie, 	Platforma e-usług publicznych	lic.	30
7	Monitoring środowiska	<p>Pozycja dotyczy wdrożenia w gminie systemu monitoringu środowiskowego obejmującego bieżące pomiary następujących czynników szkodliwych: PM2,5, PM10, PM1 w lokalizacjach na terenie gminy. Dodatkowo prowadzone będą pomiary temperatury, wilgotności, ciśnienia atmosferycznego. Dane zbierane z czujników publikowane będą na portalu eBOM oraz będą udostępniane w formie danych surowych, otwartych wszystkim zainteresowanym stronom. Przewiduje się udostępnienie danych okresowych na</p>	Platforma e-usług publicznych	zestaw	1

		portalu eBOM. System składał się będzie z dwóch (2) stacji pomiarowych oraz zintegrowanego z nimi systemu informatycznego (aplikacja dostępna w chmurze) zapewniającego ich analizę i publikację. Ponadto dane z czujników będą prezentowane w ujęciu geograficznym na podkładach mapowych.			
8	Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa	<p>Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę.</p> <p>Platforma do wykrywania i zarządzania incydentami, podatnościami i ryzykiem</p> <p>1.SOAR - Security Orchestration, Automation and Response służące do automatyzacji zarządzania i reagowania na incydenty oraz usprawnienia innych procesów zarządzania bezpieczeństwem.</p> <p>a)Uporządkowana praca ludzi – proces zarządzania incydentami (Workflow) odbywa się etapowo, zgodnie z obowiązującymi standardami (m.in. ISO/IEC 27035)</p> <p>b)Unifikacja narzędzi - jedna graficzna konsola zawiera wszystkie narzędzia i informacje potrzebne do wyjaśniania i obsługi incydentów</p> <p>b) Automatyzacja pracy ludzi - gotowe do użycia scenariusze obsługi incydentów (Playbooki) dla wielu rodzajów incydentów</p> <p>d) Integracja narzędzi i źródeł danych Plabooki automatycznie uruchamiają narzędzia i pozyskują dane ze źródeł zewnętrznych (m.in. Threat Intelligence)</p> <p>e) Priorytetyzacja biznesowa - incydenty są automatycznie priorytetyzowane w odniesieniu do ważności zasobów dla organizacji (tzn. wspomaganych procesów, wrażliwych informacji)</p> <p>f) Świadomość skutków incydentu - proces obsługi incydentów odbywa się ze świadomością ryzyka (norma ISO/IEC 27005) i biznesowych skutków naruszenia bezpieczeństwa</p> <p>g) Zunifikowane zarządzanie podatnościami – współpraca z narzędziami Vulnerability Assessment i CVE oraz zintegrowane narzędzia Workflow i Playbook do zarządzania podatnościami</p>	Cyberbezpieczeństwo	lic.	1



h) Symulacja i wizualizacja zagrożeń - analiza incydentów i podatności jest wspomagana za pomocą graficznych narzędzi symulacji ataków i innych zagrożeń

i) Metryki efektywności z kontekstem biznesowym - narzędzia obliczają kluczowe wskaźniki efektywności KPI (key performance indicator) oraz kluczowe wskaźniki ryzyka KRI (key risk indicator)

2. SIEM - Security Information and Event Management zaprojektowane pod kątem spełnienia współczesnych wymagań bezpieczeństwa umożliwiające szybkie wykrywanie incydentów i innych zagrożeń

a)Wiele metod detekcji – reguły korelacji SIEM, analiza behawioralna użytkowników i systemów (UEBA), Threat Intelligence

b)Dynamiczne reguły SIEM – reguły korelacji zdarzeń automatycznie dostosowują się do zmian sieci i systemów wykrywanych za pomocą funkcji Auto-Discovery

c) Kontekst biznesowy – analiza logów w SIEM odbywa się w kontekście aktualnego ryzyka dla procesów organizacji i wrażliwych informacji

d) Szeroki zakres analizy – SIEM poddaje analizie zdarzenia bezpieczeństwa (logi), aktualne podatności, informacje Threat Intelligence oraz oszacowane wielkości ryzyka

c)Repozytorium zdarzeń – specjalistyczna baza plikowa do długoterminowego składowania i szybkiego wyszukiwania zdarzeń bezpieczeństwa - Wiele metod odczytu logów – Syslog, e-mail, Windows Event Forwarding, a także możliwość odczytu logów z baz danych oraz plików płaskich

d) Graficzny edytor parserów - predefiniowany zestaw parserów może zostać rozszerzony o nowe parsery tworzone za pomocą graficznego edytora

e) Efektywność kosztowa - licencjonowanie oparte jest na rzeczywistej liczbie monitorowanych zasobów IT/licencja open na urząd - bez ograniczeń na wielkość analizowanych danych



9	Oprogramowanie do zarządzania infrastrukturą IT	<p>Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę. Zarządzanie IT dotyczy monitorowania infrastruktury znajdującej się w organizacji oraz użytkowników, którzy korzystają z jej zasobów. Odpowiednie zarządzanie zasobami informatycznymi wpływa na optymalizację pracy i obejmuje między innymi:</p> <ol style="list-style-type: none"> 1.Zdalne zarządzanie komputerami (RDP, webRTC, VNC, VPro/AMT), 2.Zarządzanie za pomocą serwera zadań, 3.Zdalną instalację, 4.Zarządzanie oprogramowaniem, 5.Serwer automatyzacji, 6.Serwer wiadomości, 7.Raporty, 8.Obsługę zgłoszeń wsparcia technicznego (HelpDesk), 9.System szkolenia pracowników (LMS), 10. Powiadomienia administracyjne. 	Cyberbezpieczeństwo	lic.	1
10	Oprogramowanie bazy danych	<p>Oprogramowanie - licencja jednostkowa. System bazodanowy (SBD) typ licencjonowany na rdzenie procesora pozwalający na pracę w środowisku wirtualizacyjnym musi spełniać następujące wymagania poprzez wbudowane mechanizmy:</p> <ol style="list-style-type: none"> 1.Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL. 2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich 	Cyberbezpieczeństwo	lic.	2

		<p>wykonywania.</p> <p>3.Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.</p> <p>4.Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.</p> <p>5.Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).</p> <p>6.SBD musi umożliwiać tworzenie klastrów niezawodnościowych.</p> <p>7.Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech: -bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD), -niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe), -klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,</p>			
11	Oprogramowanie serwerowe	<p>Oprogramowanie - licencja jednostkowa. System operacyjny będzie służył do instalacji modułów oprogramowania zakupionego i modernizowanego w ramach projektu. Pozwalający na instalację sieciowego systemu operacyjnego w środowisku wirtualnym. Zgodny z: - platformą sprzętową wirtualizacyjną. - serwerem backupu i zarządzania. - oprogramowaniem do backupu.</p>	Cyberbezpieczeństwo	lic.	2

		- oprogramowaniem dziedzinowym Oprogramowanie zostanie wykorzystane do podniesienia wersji usługi katalogowej - centralnego systemu uwierzytelnienia dla pracowników Urzędu (baza kont).			
12	Oprogramowanie do wirtualizacji	Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę. Pozycja dotyczy zakupu aktualizacji licencji na posiadany system do wirtualizacji wraz z aktualizacją wersji do najnowszej oferowanej przez producenta oprogramowania - podniesienie wersji.	Cyberbezpieczeństwo	lic.	1
13	Oprogramowanie do backupu	Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę. <ul style="list-style-type: none"> • Możliwość wykonywania kopii zapasowych pełnych wirtualnych maszyn niezależnie od systemu operacyjnego wewnątrz wirtualnej maszyny. • Możliwość definiowania harmonogramów. • Możliwość wykonania kopii zapasowej z pominięciem harmonogramu. • Możliwość odtworzenia pełnej wirtualnej maszyny. • Możliwość przywrócenia do alternatywnej lokalizacji. • Możliwość odtworzenia składników wirtualnej maszyny takich jak: o plik konfiguracyjny wirtualnej maszyny o dysk wirtualnej maszyny • Możliwość odtworzenia plików gościa bez konieczności odtwarzania pełnej wirtualnej maszyny. • Możliwość skonfigurowania backupu do zdalnej lokalizacji (dodatkowe miejsce przechowywania danych) • Oprogramowanie powinno umożliwiać współpracę z macierzami SAN (snapshoty macierzowe) - funkcjonalność może być osiągnięta poprzez aktywację licencji. 	Cyberbezpieczeństwo	lic.	1
14	Serwer	<ul style="list-style-type: none"> • Obudowa dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania. • Co najmniej dwa procesory 64 bitowe z sprzętowym wsparciem wirtualizacji. • Co najmniej 256GB RAM 	Platforma sprzętowa	szt.	2

		<ul style="list-style-type: none"> • Co najmniej 2 porty LAN 10Gbit/s. • Co najmniej 2 porty LAN 1Gbit/s. • Co najmniej 2 portowy kontroler sieci SAN do połączenia z siecią SAN lub bezpośrednio z macierzą dyskową – przepustowość 12GB każdego portu. • Co najmniej 2 redundantne zasilacze. • Co najmniej dwa dyski SSD pracujące w RAID 1 wspierane przez system wirtualizacji serwerów – o pojemności co najmniej 120GB. 			
15	Macierz dyskowa	<ul style="list-style-type: none"> • Obudowa przystosowana do zamontowania w oferowanej szafie rack 19 " wraz z zestawem szyn montażowych. • Zainstalowane co najmniej dwa, redundantne kontrolery SAS/FC. • Wspierane poziomy zabezpieczeń RAID 0,1,10,5,50,6. • Możliwość instalacji, co najmniej 180 dysków twardej (poprzez dokładanie kolejnych półek dyskowych). • Co najmniej 4 porty komunikacji z siecią SAN na kontroler – SAS 12G lub FC 16G. • Minimum 16 GB Cache na kontroler. • zainstalowane 12 szt.dysków SSD o pojemności co najmniej 1,9TB. 	Platforma sprzętowa	szt.	1
16	Firewall	<ul style="list-style-type: none"> • Urządzenia pracujące w klastrze • Możliwość łączenia w klastr Active-Active lub Active-Passive każdego z elementów systemu • możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent • Minimum 10 interfejsami miedzianymi Ethernet 10/100/1000 pracującymi niezależnie • Możliwość tworzenia interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q • Wydajność systemu Firewall min 1 Gbps • Filtr Antywirusowy. • Filtr stron WWW. • Filtr aplikacji. • Ochrona przed i wykrywanie intruzów. 	Platforma sprzętowa	szt.	1

		<ul style="list-style-type: none"> • Filtrowanie poczty e-mail. • Zapobieganie wyciekowi danych. • Filtr reputacji klienta. • VPN dla użytkownika. • VPN site-to-site. 			
17	Centralny system logów	<p>Urządzenie/System będzie zbierał logi z urządzenia firewall i przekazywał je do modułu SOC (SIEM/SOAR) - kolektora danych, celem dalszej obsługi, weryfikacji w kontekście bezpieczeństwa przetwarzania danych.</p> <p>System centralnego logowania i raportowania:</p> <ul style="list-style-type: none"> • Umożliwia centralne miejsce składowania logów ze wszystkich urządzeń bezpieczeństwa • Umożliwia generowanie raportów w trybie na żądanie oraz w trybie cyklicznym • Umożliwia wysyłanie powiadomień o zdarzeniach (email, SNMP) • Umożliwia export zgromadzonych logów do zewnętrznych systemów <p>W ramach centralnego systemu logowania, raportowania i korelacji powinny być realizowane przynajmniej poniższe funkcjonalności:</p> <ul style="list-style-type: none"> • Konfigurowalne opcje powiadamiania o zdarzeniach jak. email, SNMP • Podgląd logowanych zdarzeń w czasie rzeczywistym. • Możliwość generowania raportów w zakresie wszystkich funkcjonalności bezpieczeństwa realizowanych przez system - na żądanie oraz w trybie cyklicznym, w postaci popularnych formatów min: PDF. Raporty powinny obejmować zagadnienie dotyczące całej sfery bezpieczeństwa. • Zastosowane systemy logowania powinny umożliwiać cykliczny eksport zgromadzonych logów do zewnętrznych systemów przechowywania danych w celu ich długo czasowego składowania. • Na podstawie analizy przeprowadzonych testów w zakresie ilości logów w ciągu sekundy, zastosowany system centralnego logowania powinien umożliwiać zapis oraz analizę co najmniej 200 nowych 	Platforma sprzętowa	szt.	1

		logów/sekundę. • System powinien dysponować co najmniej 4 interfejsami Ethernet 10/100/1000 oraz powierzchnią dyskową min. 1 TB			
18	Zestaw komputerowy z oprogramowaniem	Komputer stacjonarny • Procesor: Min. 4-rdzeniowy, osiągający w teście PassMark CPU Mark wynik min. 7620 punktów • RAM: 8GB • HDD: 246 GB SSD • Grafika: Zintegrowana z płytą główną • Karta dźwiękowa zintegrowana z płytą główną; wbudowany głośnik • Karta sieciowa: 1Gb/s • Monitor: LCD kolorowy 23,8" panoramiczny 16:9 • System operacyjny • Oprogramowanie biurowe, antywirusowe	Platforma sprzętowa	szt.	26
19	Laptopy	Pozycja uwzględnia koszt zakupu laptopa dla pracowników urzędu. Urządzenia pozwolą na obsługę systemów dziedzinowych w zakresie e-usług publicznych, pracę zdalną, zdalną obsługę systemów. Parametry planowane: 1. Komputer do zastosowań biurowych, 2. Matryca min 14 cali 3. Wbudowana kamera 4. Port sieci LAN 1Gbps 5. Obsługa sieci WiFi min. 5 6. Pamięć RAM min. 16 GB RAM, 7. Dysk min. 256 GB SSD, 8. System operacyjny - licencja wieczysta 9. Oprogramowanie biurowe, antywirusowe	Platforma sprzętowa	szt.	4
20	Sprzęt e-Rada	Zestaw sprzętowy dla 22 osób (radnych w tym przewodniczący, wójt, sekretarz, skarbnik, pracownik obsługi, przewodniczący osiedli) - Centrala system konferencyjnego - 1 szt. - Mikrofon konferencyjny - 22 szt. - Zestaw mikrofonowy - 1 szt. - Kamera do transmisji - 2 szt.	Platforma sprzętowa	kpl.	1
				SUMA	80

SPECYFIKACJA USŁUG

Tytuł projektu:		"Platforma e-usług publicznych w Mieście Radymno "		
Wnioskodawca:		Miasto Radymno		
Lp.	Nazwa	Zakres usług	Jednostka miary [h, rbh]	Ilość
1	Integracja (Platforma e-usług publicznych)	Usługa obejmuje integrację wszystkich elementów oprogramowania w jeden spójny system, gdzie głównym kanałem dostępu do wszystkich funkcjonalności i e-usług będzie system eBOM. Usługa obejmuje również połączenie poszczególnych systemów dziedzinowych z węzłami autentykacji, bramkami płatnościowymi, obiegiem dokumentów, systemem ewoda, formularzami ePUAP w taki sposób, aby możliwe było realizowanie e-usług opisanych w projekcie na wskazanych poziomach dojrzałości.	rbh	200
2	Instalacja i konfiguracja (Platforma e-usług publicznych)	Usługa obejmuje wykonanie instalacji, konfiguracji oraz uruchomienia i przetestowania poprawności działania wszystkich modułów oprogramowania dziedzinowego objętych projektem oraz sprzętu komputerowego. W szczególności w ramach usługi zostaną wykonane następujące czynności: a) instalacja dostarczonego oprogramowania na infrastrukturze gminy b) wygenerowanie kont użytkowników, nadanie im odpowiednich uprawnień zgodnie z ustaleniami z gminą c) o ile to konieczne, zaktualizowanie posiadanych modułów oprogramowania do najnowszych dostępnych wersji, d) przeprowadzenie testów użytkownika na systemie roboczym i produkcyjnym celem weryfikacji prawidłowości działania, e) sporządzenie dokumentacji powykonawczej z instalacji i konfiguracji f) asysty stanowiskowe	rbh	200
3	Opracowanie procedur bezpieczeństwa informacji i przetwarzania danych	Pozycja dotyczy dostarczenie oraz wdrożenie Kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji. Usługa obejmuje analizę, projektowanie, implementację i szkolenie związane z wdrożeniem SZBI w jednostce. Celem usługi jest zwiększenie ochrony danych i informacji w organizacji na poziomie technicznym oraz organizacyjnym, zapewnienie zgodności z obowiązującymi przepisami prawnymi, poprawa ogólnego poziomu bezpieczeństwa informacji zgodnie z normami wyrażonymi w PN ISO/IEC 27001 w załączeniu. Na KSZBI będzie się składać: Dokumentacja zarządzania systemem zarządzania bezpieczeństwem informacji (uwzględniająca poniższe zagadnienia): – Zasady dotyczące korzystania z systemu zakres, zasoby, ciągle doskonalenie; – Procedury przeprowadzania audytów, zawierających wskazanie częstotliwości audytów, sposobu przygotowywania i zatwierdzania ich planów, sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników. – Procedury działań korygujących w przypadku niezgodności z wymaganiami systemu zarządzania.	rbh	120

		<ul style="list-style-type: none"> – Procedury wprowadzania działań zapobiegawczych w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemu zarządzania. – Procedury nadzoru nad dokumentami wchodzącymi w skład systemu zarządzania, zawierające zasady wersjonowania, zatwierdzania, dystrybucji, przechowywania, archiwizowania i niszczenia dokumentów. – Procedury nadzoru nad udokumentowaną informacją, określającej zasady przechowywania, archiwizowania oraz niszczenia zapisów. <p>oraz</p> <p>Dokumentacja dotycząca zabezpieczeń systemu zarządzania bezpieczeństwem informacji w obszarach (uwzględniająca poniższe zagadnienia):</p> <ul style="list-style-type: none"> – Zasady bezpiecznego przetwarzania informacji przez pracowników – Zabezpieczenie stacji roboczych – Zasady klasyfikacji informacji i postępowania z informacjami klasyfikowanymi – Zasady zarządzania dostępem do informacji, w tym nadawania, modyfikacji, odbierania uprawnień oraz przeglądu uprawnień – Zasady zarządzania dostępem do usług informatycznych, w tym usług sieciowych – Zarządzanie mechanizmami uwierzytelniającymi, w tym hasłami – Zasady publikacji informacji – Zasady wymiany danych z podmiotami zewnętrznymi – Zasady wewnętrznej wymiany danych – Zasady postępowania z nośnikami informacji, w tym składowanie i wymiana nośników oraz niszczenie informacji zapisanych na nośnikach – Zasady monitorowania przepisów prawnych związanych z zabezpieczeniem przetwarzanych informacji oraz wprowadzania zmian wynikających z obowiązków prawnych 		
4	Digitalizacja zasobów GIS oraz pozyskanie danych przestrzennych	<p>Zakres:</p> <ul style="list-style-type: none"> -Digitalizacja archiwalnych mpzp (3 mpzp z roku 1994) oraz obszarów aktualnie zmienionych przez nowe uchwały mpzp - 160 stron A4 ustaleń szczegółowych, 16 szt. A1, 2 szt. A0 załączniki graficzne -Digitalizacja rejestru wydanych decyzji wz i ulicp (od 2003 roku, około 350 wydanych decyzji wz i ulicp) - 300 decyzji wz, 50 decyzji ulicp -Digitalizacja rejestru GEZ – 70 kart A4 zabytków, 70 stron opisu -Digitalizacja wydanych decyzji o wycinkę drzew – 360 szt. -Digitalizacja rejestru przydomowych oczyszczalni ścieków - 5 szt. i zbiorników bezodpływowych - 34 szt. -Digitalizacja wydanych decyzji środowiskowych - 32 szt. -Digitalizacja deklaracji śmieciowych, tras i punktów odbioru odpadów komunalnych – tereny zamieszkałe 854 kartotek, tereny niezamieszkałe 202 kartotek -Implementacja danych GESUT na podstawie przekazanego pliku od PODGIK dla Miasta, konfiguracja symbolizacji i etykiet, opracowanie rejertu tabelicznego z odniesieniem na mapie: powierzchnia miasta 13,62 km2 	rbh	540

		<p>-Digitalizacja rejestru latarni, inwentaryzacja terenowa (do 400 latarni) - 310 oprav oświetleniowych</p> <p>-Fotorejestracja sferyczna dróg wraz z wektoryzacją danych pasa drogowego: 5740 m drogi powiatowe, 5520 m drogi krajowe, 15050 m drogi gminne</p> <p>a. system referencyjny – osie dróg z kilometrażem,</p> <p>b. oznakowanie pionowe,</p> <p>c. oznakowanie poziome,</p> <p>d. sygnalizacje świetlne,</p> <p>e. pasy drogowe</p> <p>f. elementy powierzchniowe takie jak jezdnie, chodniki, parkingi, pasy zieleni, skrajnie, skrzyżowania ścieżki rowerowe oraz inne,</p> <p>g. elementy punktowe takie jak drzewa, hydranty, studzienki i inne,</p> <p>h. elementy liniowe takie jak bariery, ekrany, krawężniki i inne.</p> <p>-Inwentaryzacja fotograficzna nagrobków na terenach cmentarzy (100 grobów), digitalizacja nagrobków, cyfrowo mapa ewidencji cmentarza, wykonanie ortofotomozaiki dla każdego cmentarza (2 cmentarzy) - 78 nowych grobów murowanych, 18 ziemnych</p>		
5	Szkolenia TiK typ I	<p>Pozycja dotyczy przeprowadzenia 3 autoryzowanych szkoleń w wymiarze 40 godzin każde przez producenta oprogramowania z:</p> <p>1.Administrowania i obsługi systemu operacyjnego (domena, usługa katalogowa) z zakresu zaoferowanego rozwiązania – oprogramowanie domenowe</p> <p>2.Systemu backupu z zakresu zaoferowanego rozwiązania – oprogramowanie do backupu</p> <p>3.Systemu wirtualizacji z zakresu zaoferowanego rozwiązania – oprogramowanie do backupu</p> <p>Urząd zamierza skierować na szkolenia 1 osobę – informatyk.</p> <p>Czas i miejsce realizacji szkoleń powinno zostać dobrane przez Wykonawcę z jednoczesną akceptacją przez Zamawiającego.</p>	rbh	120
6	Szkolenia TiK Typ II	<p>1. Wykonawca w ramach wdrożenia przeprowadzi instruktaże dla wskazanych użytkowników.</p> <p>2. Instruktaże prowadzone będą w języku polskim zgodnie z organizacją opisaną w Planie Szkoleń, przyjętym przez Zamawiającego.</p> <p>3. W ramach instruktaży dla liderów użytkowników, Wykonawca przekaże uczestnikom pełną wiedzę niezbędną do poprawnego użytkowania funkcjonalności Systemu.</p> <p>4. Instruktaże dla użytkowników należy przeprowadzić w formie instruktaży grupowych, w formie warsztatów (praca przy komputerach)</p> <p>5. Instruktaże grupowe winny się odbywać w podziale na grupy zawodowe nie więcej niż 5 osobowe. Każda grupa w wymiarze czasu co najmniej 8 godzin/dziennie.</p> <p>6. Dla przeprowadzenia instruktaży grupowych Zamawiający nieodpłatnie zapewni Wykonawcy 5 stanowisk roboczych (pochodzących z zamówienia w ramach niniejszego projektu) i odpowiednie pomieszczenie wraz z infrastrukturą transmisji danych umożliwiającą dostęp do Systemu. Odpowiedzialność za przygotowanie stanowisk do przeprowadzenia instruktaży leży po stronie Wykonawcy.</p> <p>7. Instruktaże dla administratorów Systemu przeprowadzone zostaną w jednej grupie.</p>	rbh	168

		<p>8. Wykonawca przeprowadzi szkolenia dla Użytkowników systemu w ciągu wskazanych/ustalonych dni szkoleniowych.</p> <p>9. Przeprowadzenie instruktaży zostanie potwierdzone protokołem sporządzonym w dwóch jednobrzmiących egzemplarzach, po jednym dla Zamawiającego i Wykonawcy, zawierającym:</p> <ol style="list-style-type: none"> nazwę i tematykę i czas trwania szkolenia, datę i miejsce szkolenia, imienną listę osób uczestniczących w szkoleniu, imię i nazwisko oraz specjalizację osób prowadzących szkolenie. <p>10. Protokół z przeprowadzenia instruktaży podlegać będzie zatwierdzeniu przez Zamawiającego.</p>		
7	Instalacja i konfiguracja (Platforma sprzętowa)	<p>Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Wnioskodawcę z uwzględnieniem wszystkich lokalizacji.</p> <p>2. Urządzenia, które nie są montowane w szafach teleinformatycznych np.: komputery powinny zostać zamontowane w miejscach wskazanych przez Wnioskodawcę</p> <p>3. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.</p> <p>4. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.</p> <p>5. Dla urządzeń modułarnych wymagany jest montaż i instalacja wszystkich podzespołów.</p> <p>6. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchcordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).</p> <p>7. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).</p> <p>8. Instalacja, konfiguracja i wdrożenie dostarczonego oprogramowania</p> <ol style="list-style-type: none"> systemu wykonywania backupu i archiwizacji danych. systemu serwerowego wraz z niezbędnymi usługami opisanymi oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn. monitorowania i analizy cyberbezpieczeństwa - SOC (SIEM/SOAR). zarządzania infrastrukturą IT. <p>9. Rejestracja oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Wnioskodawcy)</p> <p>10. Opracowanie dokumentacji powykonawczej.</p> <p>11. Asysty stanowiskowe.</p>	rbh	150