Opis Przedmiotu Zamówienia

dla postępowania ROS.271.12.2022

„Dostawa i wdrożenie sprzętu w ramach projektów Cyfrowa Gmina” i „Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym – Granty PPGR”

Identyfikator postępowania 68e56233-3be8-438a-9627-d63c3ea2bc38

współfinansowane przez Unię Europejską w ramach Europejskiego Funduszu Rozwoju Regionalnego, Program Operacyjny Polska Cyfrowa (POPC) na lata 2014-2020, pakiet REACT-UE

Wójt Gminy
Sławomir Kowalczyk
(-)

Zatwierdził: ……..

Świątki, 16.06.2022

Mając na uwadze nadrzędność celu jakim jest skuteczne uruchomienie planowanych rozwiązań Zamawiający zastrzega, że zadaniem Wykonawcy jest dostarczenie wszelkich niezbędnych elementów sprzętowych, oprogramowania, licencji oraz wykonanie wszystkich niezbędnych prac instalacyjnych, konfiguracyjnych i wdrożeniowych, które konieczne są do prawidłowego działania zgodnie z przeznaczeniem, nawet jeśli nie zostały one wymienione w dalszej części niniejszego dokumentu.

1.1. Wymagania ogólne

W ramach przedmiotowego zamówienia, Zamawiający wymaga dostarczenia, instalacji oraz konfiguracji sprzętu i oprogramowania systemowego oraz bazodanowego, którego parametry minimalne wskazane zostały poniżej. Zamawiający akceptuje sprzęt oraz oprogramowanie o wyższych (lepszych) parametrach użytkowych lub wykonany w nowszej technologii pod warunkiem, że produkty zaoferowane przez Wykonawcę spełniają wszystkie parametry minimalne.

Wszystkie oferowane produkty mają pochodzić z oficjalnego kanału dystrybucyjnego producenta, posiadać wszystkie wymagane certyfikaty i oznaczenia oraz spełniać wszystkie wymagane prawem normy.

Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie wcześniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by były nieużywane.

Zamawiający wymaga kompleksowego uruchomienia i zainstalowania dostarczonego sprzętu oraz oprogramowania.

1.2. Gwarancja i serwis

Zamawiający wymaga udzielenia gwarancji, terminów licencji i wsparcia technicznego, zgodnie ze złożoną ofertą oraz warunkami podanymi poniżej.

Sprzęt i licencje

1. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów lub ich autoryzowanych, w zakresie serwisu, partnerów.
2. Wykonawca dostarczy wraz z towarem dokument gwarancji, jakości sprzętu wystawiony przez siebie lub producenta urządzenia, zobowiązujący wystawcę dokumentu (gwaranta) do usunięcia wady fizycznej towaru lub do dostarczenia towaru wolnego od wad, jeżeli wady te ujawnią się w ciągu terminu obowiązywania gwarancji. Dokument wystawiony przez Wystawcę dokumentu (gwaranta) musi odzwierciedlać wykupione pakiety gwarancyjne i serwisowe u producenta lub jego autoryzowanych dystrybutorów o ile oferent nie posiada takiej autoryzacji

3. Okres gwarancji, które Wykonawca udzieli Zamawiającemu, będzie zgodny ze złożoną ofertą, lecz nie krótszy niż wyspecyfikowany dla poszczególnych urządzeń i oprogramowania.
4. Bieg okresów gwarancyjnych rozpoczyna się z dniem podpisania Protokołu Odbioru Końcowego bez uwag (zastrzeżeń).
5. Czas naprawy wyłączony będzie z okresu gwarancyjnego. Czas trwania gwarancji zostanie automatycznie wydłużony o czas trwania naprawy.
6. Wykonawca udziela Zamawiającemu (min. **24 miesięcznej**) gwarancji na bezawaryjne działanie wszelkich dostarczonych elementów.
7. W okresie gwarancji, wszelkie koszty związane z usunięciem awarii, w tym dostarczenie uszkodzonego sprzętu do punktu serwisowego, obciążają gwaranta.
8. Gwarancja obejmie wszystkie wykryte podczas eksploatacji sprzętu usterki i wady oraz uszkodzenia powstałe w czasie poprawnego zgodnego z instrukcją użytkowania.
9. Zasady eksploatacji i konserwacji urządzeń zostaną określone w przekazanej przez wykonawcę „Instrukcji użytkowania i eksploatacji urządzeń" wraz z wykazem urządzeń, które wymagają przeglądów serwisowych.
10. W przypadku awarii sprzętu, która nie została usunięta w terminie 30 dni, Wykonawca zobowiązuje się do wymiany sprzętu na nowy o parametrach nie gorszych od sprzętu uszkodzonego. Wymiana sprzętu na nowy nastąpi najpóźniej w 35 dniu od zgłoszenia.
11. Wykonawca zapewni możliwość zgłaszania awarii sprzętu w okresie gwarancji telefonicznie oraz drogą mailową w godzinach od 08.00 do 16.00 od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy. Zgłoszenie awarii po godz. 16.00 będzie traktowane, jak zgłoszenie o godz.08.00 następnego dnia roboczego.
12. Wykonawca musi podjąć czynności serwisowych w czasie nieprzekraczającym jednego dnia roboczego od momentu zgłoszenia o ile nie wymaga szybszej reakcji minimalny czas opisany w przedmiocie zamówienia.
13. W przypadku stwierdzenia wady ukrytej sprzętu (towaru) wykonawca musi wymienić go na nowy, w ciągu 21 dni roboczych od daty zgłoszenia tej wady.
14. W przypadku, kiedy Wykonawca uzna za konieczna naprawę sprzętu w serwisie, gwarant zapewni:
    1) odbiór na własny koszt wadliwego sprzętu (towaru) w terminie nieprzekraczającym 2 dni roboczych;
    2) dostawę naprawionego sprzętu na własny koszt w terminie nie przekraczającym 2 dni roboczych od dnia usunięcia awarii przez serwis, a w uzasadnionych przypadkach w terminie nie dłuższym niż 21 dni roboczych od odebrania sprzętu z siedziby zamawiającego
15. Koszt dojazdu ekipy serwisowej w ramach napraw gwarancyjnych i koszty transportu sprzętu naprawianego w ramach gwarancji pokryje wykonawca.

Inne wymagania

Oferowane przez Wykonawcę w dniu składania ofert rozwiązania, nie mogą być przeznaczone przez ich producenta do wycofania z produkcji, sprzedaży lub z wsparcia technicznego. Oferowane urządzenia muszą być przypisane w serwisie producenta do Zamawiającego.

Zamawiający wymaga, aby dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień składania ofert.

W celu potwierdzenie spełnienia przez oferowany sprzęt wskazanych w niniejszym dokumencie wymagań, Wykonawca na wezwanie Zamawiającego przedłoży szczegółowy wykaz oferowanego sprzętu, użyte do realizacji zamówienia komponenty, karty katalogowe lub inną dokumentację techniczną z zaznaczeniem na nich wyspecyfikowanych parametrów. Dodatkowo w przypadku dedykowanego montażu własnego Wykonawca przedstawi oświadczenie producenta sprzętu lub inny dokument poświadczający, że Wykonawca posiada autoryzacje producenta na dokonywanie modyfikacji konfiguracyjnych sprzętu i że taka modyfikacja nie ma wpływu na ewentualne świadczenia gwarancyjne.

Ogólne zasady równoważności rozwiązań

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.
Wykonawca odpowiedzialny jest za dostawę w pełni funkcjonujących rozwiązań opisanych w niniejszym załączniku, w tym jeżeli jest konieczne, pozyskanie niezbędnych informacji do realizacji zamówienia, zawarcie koniecznych umów itp.

Część 1:

1.1. Laptop v1 – 10 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Procesor	Procesor min. 4-rdzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej 10000 pkt. na podstawie PassMark PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Pamięć operacyjna RAM	Min. 8 GB DDR4 Możliwość rozbudowy pamięci do min. 32GB
Parametry pamięci masowej	SSD min. 500 GB Możliwość rozbudowy do konfiguracji dwudyskowej
Karta graficzna	Zintegrowana
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Stereo (2x 2W) z funkcją Dolby Audio, port słuchawek i mikrofonu typu COMBO, kamera video 720p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem klawiszy funkcyjnych na klawiaturze, przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).
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.
Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym.
Bezpieczeństwo	TPM 2.0
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - numer seryjnym komputera - ilości zainstalowanej pamięci RAM - typie procesora i jego prędkości

	- informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość ustawienia hasła Administratora - Możliwość ustawienia hasła Użytkownika - Możliwość ustawienia hasła dysku twardego - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS - Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, Bluetooth
Ekran	Matowy, matryca 15.6" +/- 0,4" z podświetleniem LED, rozdzielczość FHD 1920x1080, jasność min. 250 nitów, kontrast min. 800:1
Interfejsy / Komunikacja	3x USB 3.2 z czego min. 1 złącze Typu-C wspierające transfer danych, zasilanie notebooka (Power Delivery) i DisplayPort 1.4. 1x Thunderbolt 4 wspierające transfer danych, zasilanie notebooka (Power Delivery) i DisplayPort 1.4. Złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. 1.4b, RJ-45. Czytnik kart pamięci.
Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX 2x2 Bluetooth 5.1
Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w min. 2 stopniowe podświetlanie przycisków.
Akumulator	Min. 45Wh, pozwalający na nieprzerwaną pracę urządzenia do min. 6 godzin – załączyć test MobileMark 2018 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 30 minut od 0% do 50%.
Zasilacz	Zasilacz zewnętrzny 65W
Certyfikaty, oświadczenia i standardy	Komputer spełniający: - ENERGY STAR 8.0 - Ochronę oczu TÜV Low Blue Light - Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych - Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie bezczynności (IDLE) wynosząca maksymalnie 20 dB
Waga/Wymiary	Waga urządzenia z akumulatorem: maks. 2 kg Grubość notebooka nie większa niż: 25 mm
System operacyjny	Microsoft Windows 10 lub 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
Oprogramowanie biurowe	Oprogramowanie biurowe z licencją wieczystą zawierające minimum: • arkusz kalkulacyjny, • edytor tekstu, • program do tworzenia prezentacji, Programy wchodzące w skład pakietu muszą w 100% odwzorowywać treść i układ dokumentów doc, docx, rtf, xls, xlsx, ppt, pptx wytworzonych w posiadanych przez Zamawiającego pakietach Microsoft Office 2016. Edytor tekstu musi poprawnie odwzorowywać wszystkie elementy umieszczone w nagłówkach i stopkach dokumentów DOC oraz DOCX, obsługiwać osadzanie innych dokumentów tekstowych oraz arkuszy kalkulacyjnych. Dla wstawianych obiektów typu „wykres" musi istnieć możliwość osadzenia danych służących do utworzenia tego wykresu z możliwością ich edycji bezpośrednio z edytora tekstu lub poprzez otwarcie danych w dostarczanym arkuszu kalkulacyjnym. Edycja 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. Śledzenie zmian wprowadzonych przez użytkowników. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. 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 użycie wszystkich funkcji dostępnych

	w posiadanym przez Zamawiającego oprogramowaniu Microsoft Excel 2016. Arkusz kalkulacyjny musi zawierać (lub umożliwiać doinstalowanie bezpłatnego dodatku) oprogramowanie umożliwiające zoptymalizować wartość komórek zmienianych w celu uzyskania oczekiwanego rezultatu końcowego, przy jednoczesnym spełnieniu wszystkich zdefiniowanych parametrów oraz ograniczeń. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe ora 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. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynność. 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. Program do prezentacji musi poprawnie obsługiwać wszystkie animacje i przejścia utworzone w posiadanym przez Zamawiającego programie Microsoft Power Point 2016. Program musi umożliwiać 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, 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.
Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
Gwarancja	Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

	Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
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 Producentowi), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. ▪ Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera ▪ Infolinia wsparcia technicznego – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00

Monitor	Zastosowanie ogólne, biurowe
Typ matrycy	matowa
Rozmiar	Min. 23,8”
Kontrast statyczny	Statyczny min. 800:1
Czas reakcji (GtG)	Nie większy niż: 6ms
Jasność	Min. 250 cd/m^2
Podstawa	Stopa z regulacją wysokości, min w zakresie 20 cm.
Złącza/interfejsy	Min. 1x VGA, 1 x HDMI, lub 1 x DisplayPort, USB-C z PowerDelivery i DP do podłączenia komputera
Zasilanie	230V, 50/60Hz
Typ zasilacza	wewnętrzny
Typowe zużycie energii	Maksymalnie 25W,
Certyfikaty	CE, RoHS
Wyposażenie	Kabel zasilający, HDMI, kabel USB-C

1.2. Laptop v2 (PPGR) – 196 szt.

Zastosowanie	**Komputer przenośny, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.**
Przekątna i rozdzielczość ekranu	Ekran o przekątnej 15,6" +/- 0,4” o jasności co najmniej 220 cd/m^2, matryca matowa (Anti-Glare).
Wydajność	Procesor klasy x86 ze zintegrowaną grafiką, osiągający min. 5000 pkt w teście PassMark PerformanceTest - CPU Mark wg wyników dostępnych na stronie: https://www.cpubenchmark.net/mid_range_cpus.html Wynik nie starszy niż 3 miesiące od daty publikacji postępowania.

Pamięć RAM	Pamięć operacyjna: 8 GB DDR4
Pamięć masowa	Parametry pamięci masowej: dysk SSD o pojemności min. 250GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access). Obsługująca funkcje: DirectX 12, OpenGL 4.6.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji)
Bezpieczeństwo	Co najmniej zgodne z TPM 2.0.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki - Stereo. Min. 1 cyfrowy mikrofon wbudowany w obudowie matrycy. Kamera internetowa co najmniej HD (co najmniej 720p, 30 klatek na sekundę) trwale zainstalowana w obudowie matrycy, wyposażona w diodę LED sygnalizująca działanie kamery. Wbudowany napędu optyczny w obudowę notebooka – co najmniej nagrywarka DVD-RW.
Klawiatura	Klawiatura wyspowa układ US–QWERTY odporna na zachlapanie, minimum 104 klawisze z wydzielonym blokiem klawiatury numerycznej. Touchpad wyposażony w dwa niezależne klawisze funkcyjne.
Bateria i zasilanie	Czas pracy na baterii min. 5 godzin według dokumentacji producenta laptopa. Zasilacz o mocy min. 45 W
Waga i wymiary	Waga nie więcej niż: 3 kg Grubość laptopa po złożeniu powinna być mniejsza niż 24 mm.
Dodatkowe oprogramowanie	Oprogramowanie umożliwiające w pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu.
System operacyjny	Licencja na system operacyjny Microsoft Windows 10 lub 11, zainstalowany system operacyjny niewymagający ręcznej aktywacji za pomocą telefonu lub Internetu w firmie Microsoft. Dopuszcza się zaoferowanie innego systemu operacyjnego pozwalającego na prawidłową obsługę aplikacji napisanych dla środowiska Win32/64 bez użycia wirtualizatorów i emulatorów.
Porty i złącza / komunikacja	• RJ-45 (nie dopuszcza się stosowania adapterów) • Min. 1x USB 3.2 Gen. 2 typu USB-C z możliwością ładowania baterii laptopa oraz wyprowadzenia sygnału Display Port • Min. 2x USB 3.2 Gen. 1 (min. 1 z możliwością ładowania zewnętrznych urządzeń bezpośrednio z portu USB komputera nawet przy wyłączonym laptopie).

	• HDMI w wersji co najmniej 1.4 • Czytnik kart multimedialnych (SD, SDHC i SDXC) • Audio: port Combo mikrofon/słuchawki • Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN obsługująca łącznie standardy IEEE 802.11ac z dwiema antenami. • Bluetooth co najmniej w standardzie 5.0,
Wyposażenie dodatkowe	Mysz USB z min. 2 przyciskami i rolką
Gwarancja	Gwarancja producenta: • Koszt transportu do i z naprawy pokrywa Wykonawca, • Naprawy gwarancyjne urządzeń muszą być realizowane przez producenta notebooka lub jego autoryzowany serwis. • Zgłoszenia serwisowe drogą online (formularz online producenta notebooka), telefonicznie oraz mailem.

1.3. Antywirus – licencje – 40 szt.

W ramach postępowania Zamawiający oczekuje przedłużenia licencji posiadanego oprogramowania firmy G-Data Endpoint Protection Bussines na okres udzielonej gwarancji, lub dostarczenie oprogramowania o minimalnej funkcjonalności odpowiadającej poniższemu opisowi.

Element konfiguracji	Wymagania minimalne
	1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami 2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim. 3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi 4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog 5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 6. Wbudowana technologia do ochrony przed rootkitami. 7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 10. Możliwość skanowania dysków sieciowych i dysków

	przenośnych. 11. Skanowanie plików spakowanych i skompresowanych. 12. Możliwość dodawania wykluczeni na podstawie a. Plik b. Folder c. Rozszerzenie d. Proces e. Hash pliku f. Nazwa zagrożenia g. Wiersz poleceń h. IP/maska 13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook. 14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta. 18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 20. Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS. 21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło. 23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji: „Informacji o programie” możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do

	administratora ochrony, numer telefonu do administratora ochrony. 24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników. 25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia. 26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 28. Praca programu musi być niezauważalna dla użytkownika. 29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. 30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. 31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 32. Możliwość odblokowania ustawień programu po wpisaniu hasła 33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu 34. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie) 35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu. 36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp. 37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora. 38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows. 39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 40. Wbudowany IDS 41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego. 42. Maszyna która przejmuję rolę silnika skanującego musi działać w

	trybach redundancji lub równej dystrybucji 43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego. 44. Możliwość tworzenia list sieci zaufanych. 45. Możliwość dezaktywacji funkcji zapory sieciowej. 46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware 48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji 49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa) 50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups 51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego. 52. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać: a) Funkcję, która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji: • -Ochrony przeglądarki internetowej • -Sieć i poświadczenia • -Błędna konfiguracja systemu operacyjnego System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty/priorytety. b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk. c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie. d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

	e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach. f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie 53. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również: a) Możliwość wymuszenia funkcji DEP systemu Windows b) Możliwość wymuszenia relokacji modułów (ASLR) 1. Ochrona poczty – mechanizm pozwalający na ochronę poczty Office 365 lub Microsoft Exchange z wykorzystaniem serwera pośredniczącego. 2. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak: - Wczesny dostęp - Dostęp do poświadczeń - Wykrycie - Crimeware 3. Zarządzanie aktualizacjami oprogramowania firm trzecich 4. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Formaty plików jakie musza być możliwe do odzyskania: 3fr | ai | arw | bay | cab | cdr | cer | cr2 | crt | crw | dcr | der | dgn | dll | dng | doc | docm | docx | dwg | dxf | dxg | eps | erf | exe | indd | ini | | jpe | jpeg | jpg | mdf | mef | mrw | msg | msi | nef | nrw | odb | odc | odm | odp | ods | odt | orf | p12 | p7b | p7c | pdd | pdf | pef | pem | pfx | png | ppt | pptm | pptx | psd | pst | ptx | py | r3d | raf | rtf | rw2 | rwl | sr2 | srf | srw | tsf | wb2 | wpd | wps | x3f | xlk | xls | xlsb | xlsm | xlsx | xml | Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania. 5. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak: a) Ukierunkowane ataki b) Podejrzane pliki i ruch w sieci c) Exploity d) Ransomware

	e) Grayware 6. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego 7. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na: a) Tolerancyjny b) Normalny c) Agresywny 8. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku a) Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora b) Możliwość przesłania archiwum zabezpieczonego hasłem c) Możliwość przesłania adresu URL d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo. 9. Wbudowany sandbox musi działać w trybie monitorowania i blokowania 10. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny 11. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania. 12. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa. 13. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa min: 50MB 14. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość: a) Filtrowania zdarzeń b) Blokowania procesów c) Dodawanie procesów do czarnej listy d) Dodawanie procesów do białej listy e) Izolacja hosta f) Aktualizacja oprogramowania firm trzecich na hoście(1) g) Przesłanie pliku do Sandbox h) Sprawdzenie informacji o pliku w Google i) Sprawdzenie informacji o pliku w VirusTotal 15. Filtrowanie zdarzeń odbywa się na podstawie: a) Ocena zagrożenia od 10 do 100 punktów b) Data wykrycia

	c) Status d) ID e) Nazwa punktu końcowego f) Typ ataku a) Ransomware b) Potencjalnie niechciana aplikacja c) Malware d) Exploit e) Fileless f) Password stealer g) Downloader h) Inne i) Zdefiniowane przez użytkownika 16. Wyszukiwanie zdarzeń może odbywać się na podstawie: a) Nazwa alertu b) IP punktu końcowego c) Hash MD5 d) Hash SHA256 e) Nazwa użytkownika 17. Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem. 18. Możliwość wyświetlenia zablokowanych hashy plików. 19. Możliwość dodania własnych hashy MD5 oraz SHA256 20. Możliwość importu hashy z pliku CSV 21. Możliwość filtrowania dodanych hashy na podstawie: a) Typu hashu b) Wartości hash c) Źródło dodania d) Informacje o źródle e) Nazwa pliku f) Firma której dotyczy wpis g) Możliwość wyboru ilości wyświetlanych wpisów na jednej stronie.
Stacje robocze i serwery Windows	1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 6. Skanowanie plików spakowanych i skompresowanych.

	7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. 8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu. 9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę. 10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych. 11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. 12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików. 13. Program musi mieć wbudowany skaner wyszukiwania rootkitów 14. Możliwość odblokowania ustawień programu po wpisaniu hasła 15. Możliwość uruchomienia zadania skanowania z niskim priorytetem 16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego. 17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej. 18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem 19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym. 20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
Konsola centralnej administracji	1. Dwa typy konsoli administracyjnej: • Konsola Cloud – serwer administracyjny po stronie producenta • Konsola On-premise – lokalny serwer administracyjny 2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows. 3. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego. 4. Możliwość integracji Domeny Active Directory w obu typach konsoli. 5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych. 6. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji

	programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki). 7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi 8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego. 9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu. 10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej. 11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa. 12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej. 13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv 14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip. 15. Możliwość generowania raportu co godzinę. 16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu. 17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej. 18. Możliwość dodania etykiety do stacji roboczej. 19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej. 20. Możliwość przechowywania kwarantanny maksymalnie 180 dni 21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny. 23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej. 24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.

	25. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy. 26. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie - Zakres adresów IP/IP - Adres bramy - Adres serwera WINS - Adres serwera DNS - Połączenie DHCP sufiksów DNS - Punkt końcowy może rozwiązać hosta - Typ sieci - Nazwa hosta 27. Integracja z serwerem Syslog 28. Uwierzytelnienie dwuskładnikowe realizowane wyłącznie przez aplikację Google Authenticator 29. Możliwosc ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni 30. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem[2] 31. Funkcja pojedynczego logowania – Single Sign-on (SSO) 32. Możliwość naprawy instalacji z poziomu konsoli 33. Raport streszczający - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak: - Zarządzane punkty końcowe - najczęściej blokowane zagrożenia - Podział zagrożeń na urządzenia takie jak stacje robocze i serwery - Status incydentów bezpieczeństwa które wystąpiły - Stan modułów punktów końcowych - Ocena ryzyka firmy - Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa. - Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware 34. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak: a) Pakiety b) Sieć c) Kwarantanna d) Polityki

	e) Raporty f) Konta 35. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na okrślenie godziny kiedy te maszyny będą usuwane 36. Możliwość określenia własnego serwera NTP 37. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne. 38. Serwer centralnej administracji musi posiadać funkcje przełączenia się miedzy widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych. 39. Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych. 40. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony. 41. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego. 42. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej. 43. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów. 44. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym 45. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat. 46. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta. 47. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą. 48. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS 49. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym. 50. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni. 51. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS

	52. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1 53. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych. 54. Możliwość skanowania SSL dla połączeń RDP 55. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.
Licencje/subskrypcje	Wymagane jest dostarczenie licencji oraz subskrypcji aktualizacyjnych na minimum 60 miesięcy

Część 2:

Wymagania ogólne:

1. Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji projektowej realizacji każdego zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji umowy.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierająca opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego (platformy sprzętowej, systemowej, bazodanowej i aplikacyjnej). Dokumentacja musi zawierać wszystkie dane pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresem dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania danego elementu Systemu w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył Politykę backupu i archiwizacji zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów.

Dokumentacja musi być sporządzona w języku polskim i dostarczona w wersji elektronicznej z możliwością przeszukiwania treści.

Zawartość Dokumentacji musi być zgodna z wytworzonym Rozwiązaniem.

Zamawiający zezwala na dostarczenie dokumentacji w formie pomocy kontekstowej wbudowanej w GUI.

Dokumentacja administratora

1. Dokumentacja Administratora Rozwiązania musi opisywać kolejność czynności i zakres możliwych danych do wprowadzenia oraz sposób postępowania w sytuacjach szczególnych i awaryjnych.
2. Dokumentacja Administratora Rozwiązania powinna być dostępna w postaci elektronicznej umożliwiającej przeszukiwanie oraz odnajdywanie konkretnych tematów.
3. Dokumentacja Administratora Rozwiązania obejmować będzie, co najmniej:
   a. szczegółową (krok po kroku) instrukcję instalacji i konfiguracji Rozwiązania
   b. opis parametrów instalacyjnych i konfiguracyjnych Rozwiązania wraz z opisem dopuszczalnych wartości i ich wpływem na działanie rozwiązania,
   c. szczegółową (krok po kroku) instrukcję wgrywania nowych wersji Rozwiązania,
   d. szczegółowy opis możliwych do zastosowania ról i uprawnień wraz z ich wpływem na działania rozwiązania.
4. Zamawiający wymaga przekazania w bezpiecznej formie wszystkich loginów i haseł umożliwiających samodzielne zarządzanie wszystkimi usługami (również zadań serwisowych).

Dokumentacja powykonawcza

Wykonawca jest zobowiązany dostarczyć Dokumentację powykonawczą, która musi być sporządzona zgodnie z poniższym szablonem, przy czym szablon może zostać uzupełniony o dodatkowe elementy przez Wykonawcę:

1. Opis wdrożonych systemów i aplikacji.
   1.1. Opis systemu.
   1.2. Funkcjonalności
   1.3. Zależność pomiędzy wszystkimi elementami Rozwiązania.
2. Opis przepływu danych pomiędzy poszczególnymi Modułami wraz ze schematami graficznymi.
3. Sposób instalacji i konfiguracji Rozwiązania:
4. Wymagane licencje - wykaz niezbędnych licencji.
5. Karty gwarancyjne.

2. Szkolenia z dostarczonej infrastruktury

Szkolenia mają na celu osiągniecie odpowiedniej wiedzy z zakresu administrowania zainstalowanymi Systemami na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia.
Szkolenia są niezbędne w celu zagwarantowania osiągnięcia zakładanych efektów w projekcie.
Szczegółowy terminarz poszczególnych szkoleń będzie podlegał uzgodnieniu pomiędzy Wykonawcą a Zamawiającym.
Wykonawca przeszkoli administratora wskazanego przez Zamawiającego w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych.
Wykonawca zapewni przeszkolenie administratora wskazanego przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanego systemu. Szkolenie musi obejmować co najmniej instalację, konfigurację, obsługę narzędzi administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii.
Uzgodnieniu pomiędzy stornami podlegają:

- Poziom szkoleń w zależności od wiedzy i umiejętności osób skierowanych na szkolenia,
- Harmonogram szkoleń,
- Materiały szkoleniowe dla szkoleń grupowych,
- Protokoły odbioru zadania dot. szkoleń.

Zamawiający oczekuje, że ilość oraz program szkoleń powinny gwarantować administratorowi systemu zapoznanie się z wszystkimi funkcjonalnościami jakie system oferuje i pozwalać na bezproblemową pracę w systemie.

1. Portal urzędu (www.swiatki.pl)

Portal Urzędu stanowić będzie centralną platformę umożliwiającą interesantom sprawne nawigowanie po udostępnionych treściach statycznych i informacjach ogólnych na temat Gminy (informacje, ogłoszenia, aktualności, relacje, itp.).

1.1.1. Wymagania ogólne

1. System musi być dostępny przez przeglądarki internetowe - zarówno moduły udostępniane mieszkańcom/interesantom jak i panel administracyjny
2. System musi być zapewniać poprawne działanie dla przeglądarek: Google Chrome, Firefox, Safari, Edge -najnowszych wersji produktów (tzw. wersjach stabilnych) wydanych przez producentów na urządzeniach stacjonarnych, jak również dla przeglądarek tabletów

i telefonów komórkowych instalowanych na najpopularniejszych urządzeniach mobilnych (system iOS i Android) zgodnie z zasadami elastycznego projektowania (ang. Responsive Web Design-RWD

3. System musi zapewniać ochronę danych osobowych i informacji stanowiących tajemnicę skarbową zgodnie z obowiązującymi w tym zakresie przepisami oraz musi być zgodny z postanowieniami WCAG 2.1 (Dz.U. 2019 poz. 848).
4. Portal musi umożliwiać bezpieczne zalogowanie się przez przeglądarkę.
5. Portal mieszkańca musi być podzielony na:
   a. część zewnętrzną:
      - Ogólnodostępny portal dla Mieszkańców/Interesantów - użytkowników niezalogowanych
   b. część wewnętrzną – dla administratora systemu i pracowników urzędu.

1.1.2. System Zarządzania Treścią

1. Panel globalny Systemu Zarządzania Treścią musi pozwalać na tworzenie wielu niezależnych podstron, różniących się treściami i funkcjonalnościami. System musi pozwalać na dodawanie, edycję, konfigurację parametrów oraz usuwanie serwisów.
2. Użytkownikami panelu globalnego będą administratorzy globalni, którzy muszą mieć dostęp od reszty systemu. Użytkownicy z dostępem do panelu globalnego muszą mieć pełne uprawnienia w jego obszarze.
3. Dostęp do panelu globalnego musi odbywać się poprzez połączenie szyfrowane (SSL).
4. System musi umożliwiać tworzenie nowych podstron poprzez wypełnienie formularza lub jako kopię już istniejącej.
5. System musi pozwalać na definiowanie takich parametrów portalu jak nazwa portalu, domena portalu, administrator portalu.
6. System portalowy musi umożliwiać dodawanie administratorów o uprawnieniach pozwalających na zarządzanie kilkoma portalami wchodzącymi w skład systemu.
7. Architektura środowiska musi bazować na wspólnym serwerze plików i WWW.
8. Całe środowisko musi pracować w oparciu o wspólną bazę danych.
9. Środowisko musi bazować na systemie zarządzania treścią CMS (ang. Content Management System).
10. Konfiguracja systemu musi pozwolić na ustawienie domeny, pod którą będzie funkcjonował system i wskazanie katalogu, który uruchomi się pod tą domeną.
11. Funkcjonalności dostępne w panelu administracyjnym muszą zależeć od uprawnień jakie posiada zalogowany użytkownik.
12. Zalogowany użytkownik musi widzieć jedynie te funkcjonalności, do których ma dostęp.

Wersje językowe

13. System musi umożliwić tworzenie wielu różnych wersji językowych stron WWW.
14. Wersje językowe tej samej strony muszą być od siebie niezależne, tzn. mogą mieć różne struktury i treści.
15. W momencie produkcyjnego uruchomienia systemu, Wykonawca musi zapewnić wsparcie dla wersji polskiej oraz angielskiej uruchamianych stron internetowych. Oznacza to, że wszystkie elementy niebędące edytowalnymi z poziomu panelu administracyjnego muszą być przetłumaczone (np. labele na button'ach).

16. System musi posiadać możliwość dodawania nowych wersji językowych i wprowadzania ich tłumaczeń z poziomu panelu administracyjnego (np. labele na button'ach)
17. System musi pozwalać na powiązywanie ze sobą tych samych treści w różnych wersjach językowych.
18. W przypadku zmiany języka na podstronie, która posiada odpowiednik w wybranej wersji językowej, system musi przekierować użytkownika od razu na wybraną podstronę. W przypadku, gdy takiego powiązania nie ma, system musi przekierować użytkownika na stronę główną

Szablony graficzne

1. System musi wspierać obsługę szablonów graficznych.
2. System musi pozwalać na nadpisywania styli z katalogu głównego, stylami w katalogu konkretnego szablonu graficznego.
3. System w momencie uruchomienia produkcyjnego musi posiadać szablony graficzne dla:
    - Strony głównej,
    - Strony pojedynczej aktualności,
    - Podstrony statycznej,
4. System musi pozwalać na szybkie dodanie nowego szablonu graficznego przez administratora systemu.
5. System musi pozwalać na dodanie nowego szablonu poprzez kopię już istniejącego.
6. System musi wspierać funkcjonalność wersji graficznych serwisów.
7. W przypadku wersji żałobnej serwisów system musi wyświetlać wszystkie grafiki (wraz ze zdjęciami i miniaturkami zdjęć) w odcieniach szarości.

Multimedia

1. System musi posiadać repozytorium plików.
2. Wszystkie pliki udostępniane na witrynach systemu muszą wcześniej znaleźć się w repozytorium.
3. Repozytorium plików musi pozwalać na katalogowanie plików (tworzenie grup i podgrup) w celu zachowania porządku w danych wysyłanych na serwer.
4. System musi pozwalać na masowe dodawanie multimediów z dysku lokalnego komputera do repozytorium plików.
5. System musi przechowywać repozytorium w osobnym katalogu na serwerze, w celu prostego tworzenia kopi bezpieczeństwa wrzucanych na serwer plików.
6. System w swojej konfiguracji musi posiadać możliwość zdefiniowania typów plików możliwych do wrzucenia do repozytorium.
7. System musi pozwalać na zmianę nazw plików i katalogów.
8. System musi pozwalać na nadawanie plikom dodatkowych opisów oraz słów kluczowych.
9. W przypadku obrazów administratorzy muszą widzieć miniatury plików w postaci podglądu danego obrazu. W przypadku innych plików system musi pokazywać ikony z symbolami rozszerzeń tych plików.
10. Wszystkie dodawanie do repozytorium pliku muszą standardowo przyjmować status opublikowane.

Role i uprawnienia

1. System musi umożliwiać tworzenie stref z ograniczonym dostępem.
2. Funkcjonalności stref z ograniczonym dostępem do systemu muszą dotyczyć zarówno panelu administracyjnego jak i treści publikowanych na froncie portalu.
3. Ograniczenia w dostępie do poszczególnych stref muszą zostać rozwiązane za pomocą ról oraz grup uprawnień, gdzie:
    a. rola – zbiór uprawnień w obrębie panelu administracyjnego,
    b. grupa – struktura drzewiasta, do której należą użytkownicy.
4. Dostęp do panelu administracyjnego portalu, może mieć wyłącznie użytkownik, któremu przyznano prawo dostępu do logowania się do portalu. Taki użytkownik może być super administratorem portalu – posiada dostęp do wszystkich jego funkcjonalności lub ma dostęp wyłącznie do części opcji panelu, na podstawie uprawnień nadanych mu przez administratora.
5. System musi posiadać możliwość nadawania użytkownikom uprawnień poprzez przypisanie do roli.
6. Udostępnianie na froncie systemu treści wyłącznie dla zalogowanych użytkowników musi odbywać się poprzez wskazanie konkretnych użytkowników lub wybór grupy użytkowników.
7. System musi pozwalać na ręczne tworzenie grup użytkowników .
8. Użytkownik posiadający możliwość nadawania uprawnień w systemie, nie może nadać uprawnień wyższych niż sam posiada.

Edycja treści

1. System musi posiadać edytor treści WYSIWYG (ang. What You See Is What You Get).
2. Edytor treści systemu musi pozwalać na łatwe i intuicyjne wprowadzanie treści przez redaktorów, bez konieczności znajomości zagadnień technicznych, np. atrybutów html'a.
3. Edytor treści systemu musi posiadać możliwość trybu pracy w wersji html.
4. Edytor treści systemu nie może mieć ograniczeń co do wprowadzanych atrybutów lub znaczników kodu html.
5. Edytor treści system musi pozwalać na wstawianie linków zewnętrznych (wpisywanych ręcznie) oraz linków wewnętrznych, do istniejących stron w strukturze serwisu (wybór menu i pozycji w menu).
6. Edytor WYSIWYG dostępny w portalu musi zawierać co najmniej następujące funkcjonalności:
    - pogrubianie tekstu,
    - kursywa tekstu,
    - podkreślanie tekstu,
    - justowanie tekstu,
    - przekreślenie tekstu,
    - cytowanie,
    - podlinkowywanie / odlinkowanie tekstu,
    - wypunktowania / numerowanie tekstu,
    - umieszczanie plików do pobrania z repozytorium plików,
    - umieszczanie zdjęć z repozytorium plików,

- umieszczanie filmów z repozytorium plików,
- umieszczanie filmów ze źródeł zewnętrznych,
- umieszczanie plików audio z repozytorium plików,
- umieszczanie plików audio ze źródeł zewnętrznych,
- przeklejanie tekstu z Worda z prawidłową konwersją w locie do formatowania docelowego edytora,
- czyszczenie formatowania tekstu,
- wstawianie zdefiniowanych stylów,
- wstawanie zdefiniowanych nagłówków i paragrafów,
- wstawanie znaków specjalnych,
- wstawianie i edycja tabel (w tym wierszy i kolumn)
- możliwość cofania i przywracania wykonanych akcji.

7. System musi posiadać poniższe funkcjonalności w przypadku wstawiania zdjęć:
   - możliwość wprowadzenia tekstu alternatywnego,
   - możliwość wprowadzenia etykiety,
   - określenie odnośnika po kliknięciu (opcje: brak, lightbox, możliwość wprowadzenia adresu URL),
   - określenie wyświetlanego rozmiaru,
8. Możliwość dodania klasy CSS lub styli.
9. System musi posiadać poniższe funkcjonalności w przypadku wstawiania tabel:
   - wstawianie tabeli,
   - ustalanie właściwości tabeli - szerokość, wysokość, odstęp między komórkami, margines w komórkach, obramowanie, etykieta, wyrównanie, wybór klasy CSS, obramowanie, kolor tła,
   - usuwanie tabeli,
   - właściwości komórki - szerokość, wysokość, styl CSS, obramowanie, kolor tła,
   - scalanie komórek tabeli,
   - podział komórek tabeli,
   - wstawianie wiersza poniżej / powyżej,
   - wstawianie kolumny przed / po,
   - usuwanie wiersza,
   - usuwanie kolumny,
   - wycięcie wiersza,
   - skopiowanie wiersza,
   - wklejanie wiersza przed / po,
   - właściwości wiersza – rodzaj (head, body, footer),
   - wyrównanie, wysokość, styl CSS, obramowanie, kolor tła.
10. Edytor treści system musi pozwalać na wstawianie treści wewnątrz edytora pochodzących z innych, dodanych już w systemie modułów.
11. Umieszczanie w edytorze treści danych z innych modułów, musi obywać się poprzez tzw. [shortcodes]. Oznacza to, że z poziomu edytora system musi wstawić specjalny kod, który dopiero na froncie strony zostanie zamieniony na właściwą treść.

12. Wstawianie [shortcodes] w treść edytora musi odbywać się automatycznie. Administrator musi najpierw określić modułu, z którego chce wstawić treść, a następnie z listy dostępnych stron o tym typie modułu, wybrać właściwy.
13. System musi pozwalać na wstawianie treści z funkcjonalności:
    - galeria zdjęć,
    - galeria wideo,
    - lista plików,
    - lista stron,
    - bannery,
    - formularze,
    - mapa

Bloki treści

1. System musi pozwalać na definiowanie bloków.
2. Blok to element systemu służący do prezentacji treści.
3. System musi pozwalać na tworzenie poniższych typów bloków:
    - niezależnych (blok opisowy z edytorem WYSIWYG, możliwość wstawienia kodu html),
    - powiązanych z dowolną funkcjonalnością systemu (np. skrót aktualności, blok bannerów, slider, galeria zdjęć, mapa google).
4. System musi pozwalać na rozmieszczanie bloków w regionach dostępnych przy definicji układu strony głównej oraz podstron (drag & drop).
5. System musi pozwalać na rozmieszczanie tego samego bloku w różnych regionach, różnych układów stron.

Aktualności

1. System musi posiadać moduł aktualności, służący do prezentacji treści takich jak news'y, wydarzenia oraz informacje.
2. System musi pozwalać na kategoryzację aktualności.
3. System musi pozwalać na zawężanie listy aktualności poprzez wybór interesującej użytkownika kategorii.
4. Podstawowy widok modułu to stronicowana lista aktualności ze zdjęciem, tytułem, datą publikacji, kategorią i lead'em aktualności.
5. System musi pozwalać na podgląd szczegółów aktualności, poprzez wejście w daną aktualność z poziomu listy.
6. Na pojedynczą aktualność muszą składać się przynajmniej pola:
    - tytuł aktualności,
    - symbol aktualności (używany w odnośniku),
    - kategorie wpisu,
    - lead aktualności (skrót aktualności),
    - treść aktualności (WYSIWYG),
    - data publikacji od, data publikacji do,
    - status publikacji,
    - zdjęcia,
    - pliki do pobrania,

- pozycjonowanie.

7. System musi pozwalać na przypisanie aktualności do kilku kategorii.
8. System musi pozwalać na automatyczne przenoszenie opublikowanych aktualności do dostępnego dla internautów archiwum.
9. Przenoszenie musi być dokonywane po zadanej dacie.
10. System musi pozwalać na załączanie do aktualności plików i zdjęć. Musi się ono odbywać poprzez edytor WYSIWYG oraz poprzez osobne zakładki w aktualności. Dodane zdjęcia muszą stworzyć galerię zdjęć pod wpisem (pierwsze zdjęcie widoczne jest na liście wpisów), natomiast dodane pliku musza się znaleźć pod treścią aktualności jako pliki do pobrania.
11. Galeria zdjęć powinna pozwalać na powiększanie zdjęć poprzez kliknięcie w miniaturę. Powiększone zdjęcia muszą być prezentowana na warstwie zaciemniającej treść strony pod dużym zdjęciem.
12. System musi pozwalać na tworzenie informacji o dostępie czasowym. Publikacja aktualności od zadanej daty, wycofanie aktualności z portalu od zadanej daty.
13. Moduł aktualności musi posiadać funkcjonalność podglądu nie opublikowanych wpisów.
14. Moduł aktualności musi posiadać funkcjonalność indywidualnych ustawień SEO dla pojedynczego wpisu.
15. Moduł aktualności musi posiadać obsługę procesu zatwierdzania i publikacji.
16. Moduł aktualności musi podlegać procesowi wersjonowania wpisów.
17. Moduł aktualności musi podlegać procesowi powiązywania wersji językowych wpisów.
18. Moduł aktualności musi posiadać przynajmniej poniższe akcje, do których można nadawać uprawnienia:
    - dostęp do listy aktualności,
    - dodawanie aktualności,
    - edycja aktualności,
    - usuwanie aktualności,
    - publikacja,
    - zatwierdzanie aktualności,
    - wersjonowanie aktualności,
    - dostęp do kategorii,
    - dodawanie kategorii,
    - edycja kategorii,
    - usuwanie kategorii

1.1.3. Wymagania dotyczące instalacji sytemu

1. Wykonawca zainstaluje we własnym zasobie informatycznym i uruchomi system.
2. Podczas dokonywania odbioru zweryfikowane będą wszystkie założenia powyższego opisu.
3. Wykonawca udostępni zasoby informatyczne do utrzymania systemu na okres udzielonej gwarancji od dnia odbioru. Wymagana jest usługa utrzymania na serwerach przez ten okres. Usługa hostingu nie może ograniczać jednostki w zakresie ilości pobranych danych w miesiącu, a udostępniona przestrzeń dyskowa musi być na poziomie co najmniej 250 GB.
4. Cena oferty Wykonawcy musi obejmować koszty utrzymania infrastruktury koniecznej do utrzymania systemu przez cały okres gwarancji.

5. Wykonawca musi zapewnić minimalną przepustowość łączy na poziomie 30 Mbit/s.
6. Łącza internetowe obsługujące infrastrukturę IT muszą zapewniać dostępność usług na poziomie minimum 99%.

2. Biuletyn Informacji Publicznej dla Gminy Świątki.

W ramach działania zostanie przedłużona subskrypcja obecnie posiadanego serwisu BIP lub dostarczony serwis Biuletynu Informacji Publicznej (BIP) dla Gminy. Ponadto prace obejmą migrację danych z obecnie użytkowanych przez Gminę stron BIP, lub udostepnienie portalu archiwalnego (zgodnie z przepisami prawa) oraz świadczenie gwarancji i opieki serwisowej w okresie udzielonej gwarancji.
BIP ma umożliwiać publikowanie treści i dokumentów zgodnie z wymaganiami Ustawy o dostępie do informacji publicznej i składać się z części publicznej oraz niepublicznej.
Część niepubliczną (panel administratora) ma stanowić zestaw narzędzi umożliwiający wykonywanie określonych czynności redaktorom, moderatorom i administratorom serwisu, podczas gdy część publiczna będzie internetową stroną WWW dostępną dla ogółu internautów.
Dodatkowo wymaga się udostępnienia strony głównej serwisu WWW na której zostaną umieszczone ogólne informacje na temat gminy wraz z linkami do wszystkim stron BIP. Serwis podmiotowy BIP musi być oddzielnie zarządzany przez użytkowników posiadających uprawnienia do wskazanego podmiotu, a strona główna musi być zarządzana za pomocą narzędzi w części niepublicznej dostępnych dla uprawnionych do tego użytkowników.
Rozwiązanie umożliwia i zapewnia:

- wprowadzanie i zarządzania stronami podmiotowymi przez użytkowników podmiotu.
- serwis WWW dla podmiotu, zarządzany za pomocą jednego zestawu narzędzi w części niepublicznej.

2.1.1. Wymagania funkcjonalne dla części publicznej

1. Wszystkie wymagania opisane poniżej muszą być spełniane zarówno dla strony głównej jak i dla każdej strony podmiotowej, o ile w szczegółowym wymaganiu nie wskazano inaczej.
2. Strona główna oraz każda strona podmiotowa mają stanowić odrębne strony WWW – odrębnie zarządzalne obszary.
3. Strona główna i podmiotowa musi posiadać możliwość zarządzania strukturą menu przez uprawnionych administratorów. Kolejne elementy menu mogą być w dowolnej liczbie zagnieżdżane w istniejących elementach menu. System musi pozwalać na zagnieżdżanie elementów co najmniej do 5-go poziomu. Każdy element menu może zawierać dowolną liczbę artykułów oraz maksymalnie 1 artykuł rozprowadzający, którego treść prezentowana jest nad listą artykułów w wybranych elemencie menu.
4. Kilka elementów menu może zostać zgrupowane i nazwana łącznie – system wtenczas musi specjalnie wyróżnić treść nazwy takiej grupy w ramach menu strony (nagłówek menu).
5. Menu podczas nawigacji musi się zachowywać w sposób interaktywny i rozwijać tylko interesujące internautę podelementy menu. Wymaga się po wywołaniu każdej ze strony (główna, podmiotowa) menu rozwiniętego tylko na pierwszym poziomie drzewa. Rozwijanie

podelementów dowolnego elementu jest realizowane dopiero po jego kliknięciu. System musi także zapewniać automatyczne zwijanie niepotrzebnych rozwinięć elementów menu.

6. Każda strona musi posiadać możliwość samodzielnego zarządzania zawartością nagłówka strony i stopki strony.
7. Z każdego miejsca na stronach BIP (głównej i podmiotowych) jest dostępna główna wyszukiwarka pozwalająca na przeszukiwanie zasobów przeglądanej strony głównej lub strony podmiotowej. Podstawowa wyszukiwarka obejmuje możliwość wyszukiwania dowolnego ciągu znaków na stronie oraz w treści dołączonych załączników. Ponadto system musi udostępnić wyszukiwarkę zaawansowaną w ramach której jest możliwość uszczegółowienia zakresu wyszukiwania, w tym co najmniej określenie dat granicznych dla artykułów, słów kluczowych, osoby odpowiedzialnej za treść artykułu oraz osoby wprowadzającej treść artykułu.
8. Wyszukiwanie pełnotekstowe obejmować musi także zawartość załączników w formatach docx, doc, rtf, html, htm, pdf, txt, xml, xls, xlsx, ppt, pptx, odt, ods, odp.
9. Dla każdego elementu menu zawierającego większą liczbę artykułów system udostępniać musi wyszukiwarkę kontekstową pozwalającą na przeszukiwanie tylko w wybranym elemencie menu. Zakres kryteriów wyszukiwania musi być dostosowywany do zastosowanego szablonu artykułu w wybranym elemencie menu. Zakres ten administrator może zmieniać za pomocą narzędzi dostępnych w panelu administracyjnym.
10. Każdy element menu musi posiadać własne archiwum artykułów, których ważność się zakończyła lub które administrator/redaktor przeniósł do archiwum. Internauta w każdym momencie musi mieć możliwość wyświetlenia jego zawartości.
11. Administrator może dla elementu menu ustawić czas jego publikacji na stronie WWW z dokładnością do dnia.
12. Zawartość informacyjna artykułów, układ i zawartość listy artykułów w danym elemencie menu jak również widok pełnej treści artykułu jest wyświetlana w oparciu o szablony artykułów.
13. System musi pozwalać na swobodne zarządzania polami szablonu artykułu. Lista dostępnych pól obejmuje co najmniej: pole tekstowe, pole treści, pole rozwijane, pole lokalizacji (3 listy rozwijane pozwalające na wskazanie województwa, powiatu oraz gminy w ramach wybranego powiatu), pole opcji, pole wyboru, pole treści z zaawansowaną edycją tekstu XHTML, pole daty, plik graficzny.
14. Dla każdego ww. pola musi być możliwe określenie tekstowej etykiety w formularzu, wymagalności, wartości domyślnej, rodzaju przechowywanych danych (tekst, data, liczba) oraz treści podpowiedzi dla redaktora wprowadzającego dane.
15. Poza swobodnie zarządzanymi w ramach szablonu polami, system musi pozwalać dla każdego artykułu na wprowadzanie:
    a. Tytułu artykułu
    b. Czasu publikacji z dokładnością do sekundy
    c. Czasu realnego/rzeczywistego wytworzenia informacji publicznej.
    d. Daty przeniesienia artykułu do archiwum
    e. Danych osoby odpowiedzialnej za treść informacji publicznej
    f. Słów kluczowych związanych z artykułem
    g. Treści wstępu do pełnej treści artykułu – nagłówek wiadomości.
16. Narzędzie do projektowania prezentacji treści artykułu dla każdego szablonu musi być narzędziem klasy WYSIWYG, pozwalającym na tworzenie treści w dowolnym układzie przy

użyciu wszystkich elementów formularza, metryki i treści artykułu, a także stałych treści dla danego szablonu.

17. Narzędzie do projektowania listy artykułów danego szablonu musi pozwalać na określenie:
    a. Elementów za pomocą których internauci mogą wyszukiwać kontekstowo w danym elemencie menu spośród wszystkich elementów składowych artykułów.
    b. Elementów po których możliwe jest przez internautę filtrowanie artykułów oraz ich sortowanie wszystkich elementów składowych artykułów.
    c. Domyślnego sortowania listy artykułów.
18. System musi pozwalać na stworzenie szablonu dostępnego tylko dla jednego dowolnie wskazanego podmiotu.
19. System musi posiadać wbudowany edytor WYSYWIG charakterystyczny dla systemów klasy CMS.
20. Edytor WYSYWIG musi umożliwiać formatowanie treści przez redaktorów bez znajomości technik programowania oraz kodu HTML w zakresie: pogrubienia czcionki, pochylenia czcionki, podkreślenia czcionki, zmiany koloru czcionki, wprowadzenia listy numerowanej, wprowadzenia listy punktowanej, wprowadzenie linku (hiperłącza) z możliwością przekierowania na inny adres strony www, adres e-mail, plik do pobrania z repozytorium plików, dodania obrazów w treści.
21. System musi udostępniać możliwość prezentowania artykułu w wielu elementach menu jednocześnie, o ile oba elementy menu wyświetlają artykuły zbudowane w tym samym szablonie.
22. System umożliwia dla każdego artykułu dodanie dowolnej liczby załączników. Pliki załączników mogą być bezpośrednio dodawane z dysku lokalnego do danego artykułu jak również z wykorzystaniem repozytorium plików. Opcja dodawania plików musi umożliwiać dodanie kilku plików jednocześnie poprzez wskazanie ich lokalizacji na dysku lub poprzez opcję drag&drop (przeciągnij i upuść) System musi automatycznie rozpoznawać, iż dodawane pliki są plikami graficznymi i proponować dla tych plików prezentowanie ich części publicznej w postaci galerii zdjęć. Galeria zdjęć musi być umieszczona w postaci miniatur bezpośrednio pod treścią artykułu. Kliknięcie na dowolną miniaturkę musi powodować przeglądanie zdjęć w postaci galerii zdjęć z dodatkowymi narzędziami pozwalającymi na przewijanie pomiędzy kolejnymi obrazkami dołączonymi do artykułu w ramach galerii.
23. System umożliwia przeszukiwanie treści plików z poziomu panelu administratora w celu ułatwienia wyszukiwania interesującego załącznika.
24. System automatycznie gromadzi i przetwarza metadane dla załączników i prezentuje je na stronie WWW. System pozwala na pobranie w postaci spakowanego pliku archiwum wszystkich plików załączników dołączonych do artykułu.
25. System podczas dodawania/edycji artykułu musi pozwalać na podgląd treści artykułu.
26. System musi umożliwiać dodawanie do artykułu okien dodatkowych – wyświetlanych na stronie WWW w prawej części treści artykułu w postaci boksów. W ramach funkcjonalności system musi umożliwiać dodawanie dowolnej liczby okien dodatkowych. Każde okno dodatkowe może przechowywać dowolny hipertekst.
27. Każda edycja artykułu i opublikowanie zmian dokonanych w jego treści powoduje dodanie w bazie nowej wersji artykułu. Internauta podczas przeglądania najnowszej wersji artykułu musi mieć możliwość podejrzenia listy poprzednich wersji artykułu oraz wyświetlenia ich zawartości. System ponadto dla każdego artykułu wyświetla metrykę obejmującą informacje

o czasie wytworzenia, realnego czasu wytworzenia informacji publicznej, publikacji i przeniesienia do archiwum, a także dane osoby dodającej artykuł i odpowiedzialnej za jego treść.

28. Podczas przeglądania dowolnej wcześniejszej niż najaktualniejsza wersji artykułu system musi wyraźnie informować internautę, iż przegląda wersję nieaktualną. System musi wraz z tą informacją oferować przejście do najnowszej jego wersji.
29. Dla każdego artykułu musi istnieć możliwość wprowadzenia dowolnej liczby nazwanych powiązań z innymi artykułami. Powiązanie (zwane dalej także relacją) musi rozróżniać co najmniej status artykułu w stosunku do powiązywanego, nazwę relacji oraz jej kierunek. Np. artykuł z treścią uchwały o zmianie w budżecie 'zmienia' artykuł z treścią uchwały budżetowej. Istniejąca relacja pomiędzy artykułami musi być prezentowana z poziomu obu powiązywanych artykułów. System nie może ograniczać liczby i rodzaju nazwanych relacji przypisywanych artykułowi. Administrator musi mieć możliwość swobodnego zarządzania centralnym słownikiem relacji istniejących w systemie.
30. Narzędzie do zarządzania artykułami musi wydzielać co najmniej następujące listy artykułów:
    a. Artykuły aktualne – lista w układzie drzewa odpowiadającemu menu zawierająca artykuły publikowane w danym momencie wraz z ich wszystkimi poprzednimi wersjami.
    b. Artykuły archiwalne – lista w układzie drzewa menu zawierająca artykuły przeniesione do archiwum wybranego elementu menu.
    c. Artykuły usunięte – lista w układzie drzewa menu zawierająca artykuły usunięte wybranego elementu menu.
    d. Artykuły nieopublikowane – lista zawierające artykuły oczekujące na zatwierdzenie do publikacji przez uprawnionych użytkowników.
    e. Artykuły robocze – lista artykułów roboczych, tworzone automatycznie co ustalony interwał czasowy oraz zapisane jako robocze decyzją redaktora.
31. System w stosunku do artykułów, przy uwzględnieniu statusu artykułu umożliwia:
    a. Dodawanie nowych artykułów.
    b. Edycję artykułów.
    c. Usunięcie artykułów. Usunięcie nie może powodować fizycznego usunięcia treści lecz oznaczenie artykułu statusem 'usunięty' i wyświetlenie go na liście usuniętych.
    d. Przywrócenie artykułu.
    e. Archiwizację artykułu oraz przywrócenie go do artykułów aktualnych.
    f. Skopiowanie treści artykułu jako nowego do wybranego elementu menu.
    g. Porównanie treści dwóch dowolnych wersji wybranego artykułu z oznaczeniem przez system treści nowododanych oraz usuniętych pomiędzy nimi.
32. Moderator nie akceptując treści do publikacji może skierować artykuł do redaktora go tworzącego.
33. System powinien umożliwić redaktorowi zmianę moderatorów artykułu bez jego edycji, w przypadku gdy nie został on jeszcze odrzucony lub zatwierdzony do publikacji.
34. Dla wskazanych przez administratora elementów menu, redaktor wprowadzając artykuł musi mieć możliwość włączenia systemu komentarzy dla artykułu przez internautów. Wprowadzone przez internautów komentarze muszą przed publikacją być zatwierdzone przez uprawnionych użytkowników.
35. System dla każdego artykułu musi oferować internaucie szereg narzędzi, w tym co najmniej:
36. Możliwość wysłania wiadomości przez formularz kontaktowy powiązany z artykułem. Lista formularzy kontaktowych jest dowolnie zarządzana przez administratora, na który składa się

dowolna liczba pól różnego rodzaju. Wysyłka formularza musi być zabezpieczona mechanizmem CAPTCHA. Każdy formularz kontaktowy musi być powiązany z co najmniej 1 adresem email na który to jest wysyłana treść wprowadzona przez internautę.

37. Możliwość polecenia artykułu znajomemu – funkcjonalność wysyłająca link z komentarzem wprowadzonym przez internautę na wskazany przez niego adres email. Formularz także musi być zabezpieczony mechanizmem CAPTCHA.
38. Możliwość pobrania treści artykułu w formacie PDF i XML.
39. Możliwość wydrukowania treści artykułu.
40. Dla każdej listy artykułów w menu system musi oferować internaucie:
    a. Pobranie listy artykułów w pliku XML.
    b. Subskrypcję kanału RSS powiązanego z danym elementem menu zawierającym wskazaną listę.
    c. Możliwość zmiany liczby artykułów wyświetlanych na liście artykułów.
41. Sortowanie i filtrowanie za pomocą pól opisujących artykuł (metadanych i pól formularza danego szablonu). Lista pól, po których możliwe jest sortowanie i filtrowanie jest konfigurowalna przez administratora oddzielnie dla każdego szablonu. System musi prawidłowo sortować po polu zawierającym tylko liczby.
42. Możliwość zmiany liczby artykułów wyświetlanych na liście artykułów.
43. System pod menu musi zawierać bezpośrednie linki do 5 ostatnio dodanych artykułów dla każdej ze stron.
44. System musi udostępniać narzędzie pozwalające na przeglądanie listy wszystkich zmian w treści publikowanych artykułów z możliwością jej przeglądania za dowolny przedział czasu.
45. System musi zawsze, na każdej stronie prezentować ścieżkę wg elementów menu w którym znajduje się aktualnie wyświetlana treść strony (ang. breadcrumbs). W przypadku strony podmiotowej systemu w tym zakresie musi uwzględniać prezentowanie kontekstu podmiotu.
46. System musi umożliwiać prezentację w formie artykułu aktu prawnego zawartego w pliku ZIPX.
47. Administrator musi mieć możliwość dodawania dowolnej liczby wersji językowych strony, wraz z możliwością przetłumaczenia wszystkich elementów stałych strony na wybrany język. Administrator podmiotu może uruchomić stronę podmiotową w języku wcześniej udostępnionym przez administratora globalnego.
48. System musi udostępniać narzędzia newslettera systemowego. Newsletter systemowy wysyła wiadomości mailowe z informacją o zmianach na stronach BIP w wybranych elementach menu.
49. Administrator zarządzając elementami menu ma możliwość udostępnienia dla niego newslettera systemowego.
50. System musi posiadać zestaw kalkulatorów dostępnych z pozycji menu: „Usunięcie drzew, krzewów, zniszczenie terenów zieleni", „Kalkulator wynajmu dróg", „Kalkulator opłat za zezwolenie na sprzedaż alkoholu" wraz z możliwością ich konfiguracji po stronie administracyjnej.
51. Każda strona podmiotowa BIP musi być dostępna zarówna z poziomu strony głównej BIP jak i pod bezpośrednim adresem URL.
52. Strona publiczna musi być stroną responsywną, a więc taką która dostosowuje swoją zawartość do urządzenia na której jest wyświetlana, ze szczególnym uwzględnieniem rozdzielczości ekranów urządzeń mobilnych.

53. BIP musi pozwalać na osadzenie w treści dowolnego artykułu mapy (np. googlemaps lub podobnych) z możliwością oznaczenia na niej dowolnej liczby dowolnych obiektów np. nieruchomości stanowiących oferty inwestycyjne. Aplikacja musi umożliwiać skonfigurowanie domyślnego przybliżenia dla mapy oraz punktu centralnego wyświetlanego kawałka mapy osadzonego na stronie.
54. System musi posiadać wbudowane repozytorium plików składającej się z samodzielnie budowanej struktury katalogów oraz z katalogów z załącznikami dodawanymi bezpośrednio do artykułów.
55. System musi umożliwiać usuwanie bezpowrotne plików z repozytorium. W przypadku ich wcześniejszego użycia w jakimkolwiek artykule to w jego miejsce musi zostać umieszczona wyraźna informacja o usunięciu pliku i powodzie jego usunięcia.

2.1.2. Wymagania funkcjonalne dla części publicznej – tylko dla strony podmiotowej

1. Aplikacja musi umożliwiać włączenie na stronie www:
   a. Licznika odwiedzin strony
   b. Linku do formularza z możliwością zadania pytania.
   c. Prezentowania listy zapytań i udzielonych odpowiedzi na najczęściej zadawane pytania.
2. Moduł ankiet musi pozwalać na definiowanie pytań, dla których odpowiedź może stanowić:
   a. Tekst otwarty.
   b. Datę.
   c. Liczbę.
   d. Wskazanie pozycji na liście jednokrotnego wyboru.
   e. Wskazanie pozycji na liście jednokrotnego wyboru z otwartą możliwością wprowadzenia tekstu.
   f. Wskazanie pozycji na liście jednokrotnego wyboru z komentarzami
   g. Wskazanie pozycji na liście wielokrotnego wyboru.
   h. Wskazanie pozycji na liście wielokrotnego wyboru z otwartą możliwością wprowadzenia tekstu.
   i. Wskazanie pozycji na liście wielokrotnego wyboru z komentarzami
   j. Ranking dostępnych opcji – ułożenie ich w odpowiedniej kolejności.
   k. Macierz opcji i wartości.

2.1.3. Wymagania dotyczące panelu zarządzania

1. Aplikacja pozwala na zarządzania użytkownikami panelu administracyjnego. W panelu zarządzania musi być prezentowana ostatnia data zalogowania użytkownika.
2. Aplikacja musi pozwalać na wyszukiwanie użytkowników.
3. Aplikacja musi pozwalać na dodawania użytkowników z kontem czasowym – ważnym i aktywnym tylko w zaplanowanym z góry okresie.
4. Aplikacja pozwala na zarządzanie uprawnieniami do każdego modułu systemu.
5. Uprawnień muszą być hierarchiczne. Aplikacja pozwala grupować uprawnienia w dowolne zestawy i przydzielać je użytkownikom. Uprawnienia mogą być przydzielane także w sposób jednostkowy.
6. Aplikacja musi pozwalać na określenia zamkniętego katalogu formatów plików przyjmowanych jako załączniki do artykułów.

7. Aplikacja musi umożliwiać sterowanie dostępem do każdego elementu menu w zakresie (tzw. ACL – Access Control List):
   a. Dodawania artykułów
   b. Edytowania artykułów
   c. Usuwania artykułów
   d. Zarządzania danym elementem menu, w tym dodawania podmenu.
8. Dostęp do elementu menu musi być nadawany każdemu użytkownikowi.
9. Aplikacja w zakresie konfiguracji musi pozwalać co najmniej na:
   a. Włączenie statystyk Google Analytics lub równoważnych.
   b. Zarządzenie zawartością stopki i nagłówka strony za pomocą edytora WYSIWYG. Możliwość umieszczania w stopce dowolnych treści, linków i obrazków. Oddzielnie dla wersji mobilnej.
   c. Określania długości sesji zalogowanego użytkownika.
   d. Zarządzanie treścią zgody na umieszczania ciasteczek na komputerze lokalnym.
   e. Zarządzanie autoryzacją użytkowników panelu zarządzania co najmniej w zakresie: możliwości logowania za pomocą certyfikatów, minimalnej liczby znaków hasła, minimalnej siły hasła, maksymalnej liczby nieudanych prób logowania, liczby minut blokady konta po przekroczeniu liczby błędnie wprowadzonych haseł, liczby dni co które system wymusza zmianę hasła, liczbę niepowtarzalnych ostatnich haseł.
   f. Zarządzanie treścią strony logowania do panelu zarządzania.
   g. Zmianę dopuszczalnej wielkości dołączanych plików jako załączniki.
   h. Zarządzenia pomocą przeznaczoną dla klienta urzędu oraz dla administratorów/redaktorów.
10. Aplikacja musi posiadać wbudowany dziennik zdarzeń z czynności wykonywanych przez redaktorów i administratorów.
11. Aplikacja musi umożliwiać konfigurację stawek do wyliczeń dla udostępnionych kalkulatorów w podziale na lata.
12. Aplikacja musi pozwalać administratorowi na tworzenie szablonów dla treści systemowych wiadomości dotyczących treści wiadomości mailowej z powiadomieniem i treścią wypełnionego formularza kontaktowego, treści newslettera, potwierdzenia z zapisania się do newslettera, potwierdzenia wypisania z newslettera, treści polecenia artykułu znajomemu, treści powiadomienia administratora o błędnej walidacji HTML treści artykułu.
13. System musi wysyłać powiadomienia wewnętrzne systemowe w przypadku: aktualizacji szablonu w określonym elemencie menu poprzez przesłanie informacji o zablokowaniu i odblokowaniu aktualizowanej pozycji, przekazania artykułu do akceptacji dla wskazanych adresatów, zaakceptowaniu artykułów.
14. Aplikacja musi umożliwiać administratorom tworzenie i wysyłkę powiadomień wewnętrznych zwykłych.
15. Powiadomienia mają być kierowane do pojedynczych użytkowników jak również grup określonych poprzez role systemowe.
16. System musi umożliwiać określenie czy dane powiadomienie jest priorytetowe. Jeżeli tak, to okno ze specjalnie oznaczoną wiadomością jest automatycznie wyświetlane u adresata po otrzymaniu powiadomienia. Użytkownik musi mieć dostęp do swoich odczytanych i nieodczytanych powiadomień z poziomu jednego okna.

17. System musi umożliwiać wgląd we wszystkie wysłane wiadomości wraz z możliwością weryfikacji czy dane powiadomienie zostało przez odbiorcę odczytana.
18. System musi umożliwiać dla plików wgrywanych do repozytorium definiowanie typów plików wraz ich identyfikatorem MIME.
19. System musi umożliwiać import plików. Zawarta treść w pliku zostanie zaprezentowana w formie artykułu opartego o odpowiednio przygotowany szablon.
20. W przypadku szablonów przeznaczonych pod publikację danych na podstawie plików musi istnieć możliwość skonfigurowania schematu mapowania pól metryki.

2.1.4. Dostępność

1. Strona www musi spełniać wymagania WCAG 2.1 co najmniej na poziomie AA.
2. BIP musi udostępniać możliwość:
   a. Powiększenia wielkości tekstu na stronie.
   b. Przełączenia się na tryb wysokokontrastowy na stronie www.
3. BIP musi obsługiwać powszechnie stosowane skróty klawiszowe uruchamiające:
   a. Wersję wysokokontrastową strony
   b. Zmianę wielkości tekstu
   c. Mapę strony – generowaną automatycznie
   d. Powrót do strony startowej
   e. Wyszukiwarkę główną
4. Strona www musi być poprawnie wyświetlane na urządzeniach mobilnych z prezentacją wszystkich dostępnych na stronie treści. Dla małych rozdzielczości ekranu wymaga się prezentowania innego układu strony, w której na górze znajduje się rozwijane menu a treści prezentowane są u dołu strony w wersji mobilnej.
5. BIP musi umożliwiać skonfigurowanie odrębnej stopki i odrębnego nagłówka strony dla widoku mobilnego (inna zawartość).

2.1.5. Wymagania niefunkcjonalne

1. BIP musi być w pełni dostępny poprzez przeglądarkę internetową. Wymaganie dotyczy zarówno części publicznej jak i panelu zarządzania. Część publiczna oraz panel muszą stanowić odrębnie działające aplikacje – nie jest dopuszczalne edytowanie treści strony bezpośrednio na jej stronie.
2. Interfejs systemu musi być zaprojektowany przy wsparciu nowoczesnych technologii internetowych, w tym być obsługiwany przez co najmniej:
   a. Microsoft Edge
   b. Mozilla Firefox od wersji 24
   c. Google Chrome od wersji 30.
3. BIP musi działać w technologii trójwarstwowej z wydzielonymi warstwami: bazodanową, aplikacyjną i kliencką, przy czym w warstwie klienckiej może istnieć tylko kod interpretowany przez przeglądarkę internetową.
4. Wszystkie dane muszą być przechowywane w bazie danych. Jeśli pliki są przechowywane poza bazą danych to muszą być jednoznacznie z nią powiązane np. poprzez obliczanie sumy kontrolnej plików i sprawdzanie jej przy każdej próbie użycia pliku. Mechanizm ma zabezpieczać przed nieautoryzowaną podmianą plików.
5. System musi działać w oparciu o kodowanie UTF-8 i język polski.

2.1.6. Wymagania dotyczące instalacji sytemu

7. Wykonawca zainstaluje we własnym zasobie informatycznym i uruchomi system BIP.
8. Podczas dokonywania odbioru zweryfikowane będą wszystkie założenia powyższego opisu dotyczące BIP.
9. Wykonawca udostępni własne zasoby informatyczne do utrzymania systemu BIP na okres udzielonej gwarancji od dnia odbioru. Wymagana jest usługa hostingu przez ten okres oraz złożenia oferty dalszego hostingu po upływie okresu gwarancyjnego. Usługa hostingu nie może ograniczać jednostki w zakresie ilości pobranych danych w miesiącu, a udostępniona przestrzeń dyskowa musi być na poziomie co najmniej 200 GB.
10. Cena oferty Wykonawcy musi obejmować koszty utrzymania infrastruktury koniecznej do utrzymania BIP przez cały okres gwarancji.
11. Wykonawca musi zapewnić minimalną przepustowość łączy na poziomie 30 Mbit/s.
12. Łącza internetowe obsługujące infrastrukturę IT muszą zapewniać dostępność usług na poziomie minimum 97%.

2.1.7. Wymagania dotyczące migracji danych z użytkowanych przez Gminę stron podmiotowych BIP

1. Wykonawca zmigruje dane do systemu BIP ze stron podmiotowych BIP.
2. Wykonawca ma za zadanie przenieść dane do docelowego systemu.
3. Wykonawca przed udostępnieniem systemu produkcyjnego musi przedstawić wersję testową BIP z przeniesionymi danymi do weryfikacji przez Gminę, a po jej zatwierdzeniu – przenieść dane do systemu produkcyjnego.
4. Migracja danych musi obejmować co najmniej:
   a. Strukturę menu
   b. Artykuły
   c. Użytkowników i uprawnienia.
   d. Podstawową konfigurację
5. Wykonawca na podstawie wytycznych Zamawiającego skonfiguruje i uruchomi systemy do pracy.
6. Zgłoszenie serwisu BIP do rejestru bip.gov.pl