Opis Przedmiotu Zamówienia

dla postępowania ROS.271.14.2022

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

Identyfikator postępowania 2b32304a-2288-4e55-9f3c-99ac7c92b5d8

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

Świątki, 25.07.2022

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
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
Waga/Wymiary	Waga urządzenia z akumulatorem: maks. 2,5 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.. W przypadku uszkodzenia lub awarii dysku twardego w okresie gwarancji, zamawiający wymaga aby uszkodzony dysk został w miejscu u zamawiającego. Wszelkie napraw odbywać się będą w siedzibie zamawiającego.
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. 2 X USB – A, 1x VGA, 1 x HDMI, lub 1 x DisplayPort, USB-C z PowerDelivery min 60 Watt 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 rozdzielczości FHD WLED (1920x1080) i jasności co najmniej 250 cd/m^2, matryca matowa (Anti-Glare). Metalowe zawiasy.
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: min 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
Bezpieczeństwo	Zintegrowany z płytą główną układ zgodny 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.
Klawiatura	Klawiatura wyspowa układ US–QWERTY Touchpad
Bateria i zasilanie	Czas pracy na baterii min. 6 godzin według dokumentacji producenta laptopa.
Waga i wymiary	Waga nie więcej niż: 3 kg Grubość laptopa po złożeniu powinna być mniejsza niż 30 mm
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. 3x USB 3.2 Gen. 1 (min. 1 z możliwością ładowania zewnętrznych urządzeń bezpośrednio z portu USB komputera nawet przy wyłączonym laptopie). • HDMI • Audio: port Combo mikrofon/słuchawki • Karta sieciowa LAN 10/100/1000 Ethernet RJ-45 zintegrowana z płytą główną. • 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,
Mysz	Mysz USB z min. 2 przyciskami i rolką
Gwarancja	Gwarancja producenta: • Naprawy gwarancyjne urządzeń muszą być realizowane przez producenta notebooka lub jego autoryzowany serwis. • Naprawa ma się odbywać na miejscu u klienta • 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.
Gwarancja	Wymagane jest dostarczenie licencji oraz subskrypcji aktualizacyjnych w formie gwarancji 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.

Portal urzędu (www.swiatki.pl). Usługa ma być świadczona wraz z aktualizacją i opieką autorską w formie gwarancji na okres minimum 60 miesięcy

1. Wymagania dla każdego projektu graficznego usługi chmurowej – serwisu www.

1) Projekt serwisu www musi uwzględniać zasady UI oraz UX, a także WCAG 2.1 dla całego układu serwisu www oraz rozmieszczenia elementów, jak również w kwestii zastosowanych czcionek, kontrastu elementów graficznych oraz tła itp.
2) Projekt graficzny serwisu www musi być opracowany dla różnego rodzaju wielkości ekranów, aby zapewnić responsywność.
3) Rozdzielczość dla wersji desktop szerokość wyświetlanego kontentu to 1600px, ale całość serwisu wyświetlana jest na 100% ekranu.

4) Zastosowany kontrast zgodny z wytycznymi dotyczącymi dostępności treści cyfrowych (WCAG 2.1). Współczynnik kontrastu co najmniej 4,5:1 dla zwykłego tekstu i 3:1 dla dużego tekstu (co najmniej 18 punktów) lub tekstu pogrubionego.
5) Projekt powinien zapewnić dostęp do najważniejszych informacji serwisu www, w jak najmniejszej ilości kliknięć – preferowane są max 3 kliknięcia.
6) Dobór kolorystyki serwisu www będzie uzgodniony z Zamawiającym.
7) Proces projektowy serwisu www uwzględniać będzie również przygotowanie wersji żałobnej, narodowej oraz świątecznej serwisu www.

2. **Wymagania funkcjonalne dla usługi chmurowej – Portal www będzie posiadał maksymalnie następujące funkcjonalności, które mogą być uruchomione lub nie, w zależności od potrzeb:**
   1) slider aktualności, z możliwością wyłączenia przez Internautę automatycznego przesuwania się kolejnych aktualności
   2) aktualności, w tym możliwość implementowania aktualności z jednego serwisu www np. Urzędu Starostwa do innego serwisu www np. PCPR i odwrotnie – funkcjonalność moderowana; możliwość kategoryzacji aktualności np. Sportowe, Kulturalne itp.; integracja aktualności z modułem Galeria oraz Kalendarz wydarzeń
   3) kalendarz wydarzeń zintegrowany z aktualnościami,
   4) galerie zdjęć z możliwością ich przeglądania: zdjęcie następne, zdjęcie poprzednie,
   5) ruchomy pasek aktualności, z możliwością wyłączenia przez Internautę,
   6) system banerowy,
   7) pop up, z możliwością wyłączenia przez Internautę,
   8) sondę,
   9) integracja z walidatorem Wave WCAG 2.1,
   10) powiadomienia Web Push dla aktualności, z możliwością ich wysyłki w ramach panelu zarządzania,
   11) dzień tygodnia i pogodę,
   12) wykaz/katalog spraw urzędowych
   13) statystyki odwiedzin zintegrowane z Google Analytics,
   14) funkcja strony do druku dla każdej informacji tekstowej, dostępna poprzez ikonkę pod każdą informacją,
   15) funkcja udostępnienia informacji na profilu Facebook dla każdej informacji tekstowej, dostępna poprzez ikonkę pod każdą informacją,
   16) wyszukiwarka,
   17) formularz kontaktowy,
   18) deklaracja dostępności,
   19) wersja serwisu www w wysokim kontraście,
   20) powiększanie/pomniejszanie czcionki/ zwiększanie odstępów pomiędzy znakami i wersami tekstu,
   21) informacja o miejscu w strukturze serwisu internetowego, w którym znajduje się aktualnie internauta, tzw. ścieżka dostępu

3. **Wymagania dotyczące systemu CMS do zarządzania usługą chmurową - serwisem www dostępne w panelu zarządzania:**
   1) panel administracyjny w polskiej wersji językowej,
   2) system CMS musi posiadać mechanizm przekierowujący użytkownika na zaprojektowaną przez Dostawcę stronę informacji o błędzie (ERROR 404) w przypadku podania

niewłaściwego adresu strony WWW, na której znajdzie się informacja o braku szukanego adresu oraz link do strony głównej danej strony WWW,

3) dostęp do panelu administracyjnego powinien być możliwy poprzez wejście na konkretny adres strony www, za pomocą loginu i hasła, zaszyfrowany za pomocą certyfikatu SSL,
4) system CMS dostarczony przez Dostawcę musi umożliwiać zarządzanie treścią całego serwisu internetowego bez konieczności znajomości języków programowania (do obsługi ma być wystarczająca podstawowa znajomość programów do edycji tekstu, obróbki grafiki).
5) system CMS musi obsługiwać wszystkie strony serwisu internetowego oraz wszystkie bazy, rejestry, listy etc.
6) pełne zarządzanie menu, tzn. dodawanie/usuwanie zakładek i podzakładek, możliwość stworzenia minimum 3 poziomów struktury menu,
7) tworzenie linków między zakładkami i podzakładkami,
8) zarządzanie widocznością i publikacją elementów struktury,
9) możliwość podejrzenia tworzonej treści bez jej publikacji na stronie wynikowej,
10) możliwość włączenia i wyłączenia graficznej wersji żałobnej, narodowej i świątecznej serwisu,
11) łatwa, pełna edycja tekstu za pomocą WYSIWYG, w tym z możliwością:
    a. pogrubienia, kursywy, podkreślenia tekstu,
    b. wyrównania tekstu, zdjęcia, tabelki: do lewej, do środka, do prawej, równaj do prawej i lewej,
    c. skorzystania z wbudowanych styli: nagłówki od 1 do 6
    d. skorzystania z listy wbudowanych rodzajów czcionek,
    e. określenia wielkości czcionki w danym tekście,
    f. określenia koloru czcionki oraz koloru tła pod tekstem,
    g. kopiowania, wycinania i wklejania podczas edycji treści,
    h. wklejania treści z edytorów tekstu np. z MS Word,
    i. zastosowania listy numerowanej i punktowanej,
    j. zastosowania wcięcia, cofnięcia wcięcia,
    k. cofnięcia i ponowienia operacji,
    l. wstawienia i edytowania linków do: pliku, zdjęcia, adresu email, strony www – z określeniem czy w tym samym oknie, czy w nowym,
    m. wstawienia pliku graficznego w treści za pomocą przeglądaj dysk, z możliwością
        i. określenia tytułu pliku oraz opisu alternatywnego,
        ii. określenia pozycji zdjęcia względem tekstu (wyrównanie do lewej lub prawej, oblanie tekstem, pozycja zdjęcia względem tekstu)
        iii. wstawienie ramki z określeniem jej grubości,
    n. przełączenia się w tryb HTML,
    o. wstawienia filmu lub pliku audio,
    p. wstawienia tabeli z możliwością:
        i. ustawienia liczby kolumn i wierszy
        ii. określenia odległości komórek od siebie,
        iii. określenia zawartości komórki od jej ramki,
        iv. wyrównanie tabeli względem tekstu,
        v. określenie obramowania tabeli,
        vi. szerokości i wysokości
        vii. kolor ramki i kolor tła,
    q. możliwość ustawienia odstępu powyżej i poniżej wiersza,

12) dodawanie załączników, do każdej podstrony tekstowej struktury serwisu, załączony załącznik musi być prezentowany w sposób automatyczny na stronie wynikowej (bez potrzeby ingerencji osoby redagującej), zgodnie z wymogami WCAG 2.1 tj. muszą posiadać nazwę pliku, rozmiar i typ,
13) każdy plik graficzny implementowany do zawartości serwisu www musi posiadać możliwość przy jego dodawaniu, określenia jego tytułu, opisu alternatywnego za pomocą odpowiednich pól,
14) funkcjonalność umożliwiająca zarządzanie aktualnościami:
    a. zarządzanie aktualnością – dodawanie nowej, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
    b. możliwość dodawania kategorii aktualności: np. dla biznesu, finansowe, itp.
    c. wypromowanie artykułu w sliderze,
    d. dodanie danego artykułu również do kalendarza wydarzeń,
    e. możliwość podpięcia galerii, która nie jest widoczna na stronie głównej
    f. możliwość umieszczenia wybranych aktualności z jednego serwisu www w innych serwisach www i odwrotnie (serwisach www powstałych w wyniku tego postępowania, zbudowanych o tę samą technologię), moduł moderowany – użytkownik z odpowiednimi uprawnieniami decyduje czy opublikować daną aktualność w swoim serwisie www.
    g. załączanie plików, w tym:
        i. implementacja plików graficznych w tekście, które muszą posiadać możliwość kadrowania, obracania, powiększania i pomniejszania, tzw. ustawienia oblewania tekstem oraz obok tekstu z lewej i prawej – w celu uzyskania odpowiedniej kompozycji,
        ii. załączane pozostałe pliki jako załączniki – muszą być prezentowany w sposób automatyczny na stronie wynikowej (bez potrzeby ingerencji osoby redagującej), zgodnie z wymogami WCAG 2.1 tj. muszą posiadać nazwę pliku, rozmiar i typ,
15) funkcjonalność umożliwiająca zrządzanie galerią zdjęć:
    a. zarządzanie galerią – dodawanie nowej, edycja i usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
    b. dodawanie zdjęć potokowo(czyli dużej ilości plików jednorazowo) za pomocą technologii Drag& Drop,
    c. dodawanie zdjęć potokowo za pomocą opcji przeglądaj z dysku,
    d. dodawanie pojedyncze zdjęć,
    e. określenie nazwy dodawanych zdjęć lub nadanie im nazwy z danej galerii,
    f. automatyczną kompresję plików o dużej pojemności i dostosowywanie ich do optymalnych cech (rozmiar w px, pojemność w MB), w celu ich poprawnej publikacji ze względu na wysokość ekranu i szybkości ładowania na stronie www,
    g. przeglądanie zdjęć za pomocą wbudowanej przeglądarki, prezentującej zdjęcia na warstwie, umożliwiającej przechodzenie do następnego zdjęcia oraz poprzedniego, a także zamykanie okna.
16) funkcjonalność umożliwiająca zrządzanie banerami w określonych miejscach serwisu www np. polecamy, na skróty, zdjęcia w top, zdjęcie dla modułu statystycznego:
    a. zarządzanie banerami - dodawanie nowego, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
    b. możliwość linkowania do stron zewnętrznych oraz podstron serwisu,
17) funkcjonalność umożliwiająca zrządzanie sondą:

a. zarządzanie sondą - dodawanie nowego, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
b. tworzenie pytania,
c. tworzenie nagłówka sondy,
d. ustawienia opcji głosowania: wielokrotne, jednokrotne,
e. widoczność sondy od ..do,
f. widoczność wyników głosowania tak/nie,

18) funkcjonalność umożliwiająca zarządzanie – wykazem spraw:
a. dodawanie/edycja kategorii spraw np. Podatek od nieruchomości
b. dodawanie/edycja wydziałów/stanowisk
c. dodawania/edycja karty sprawy według opracowanego szablonu,

19) funkcjonalność zarządzania użytkownikami systemu:
a. lista użytkowników,
b. dodawanie i zarządzanie użytkownikami,
c. nadawanie uprawnień do poszczególnych modułów oraz funkcjonalności dla utworzonych grup,
d. możliwość tworzenia i zarządzania grupami użytkowników np. administratorzy, redaktorzy – wraz z przydzieleniem ich dostępu do określonych modułów, funkcjonalności,
e. możliwość odblokowywania zablokowanych użytkowników z powodu błędnego logowania,

20) funkcjonalność integracji z kontem Google Analytics w celu uzyskania szczegółowych statystyk odwiedzalności serwisu.

21) funkcjonalność SEO – w celu określenia podstawowych danych serwisu, podlegających indeksowaniu przez wyszukiwarki internetowe, umożliwiająca co najmniej:
a. określenie pola Title (tytuł),
b. określenie pola Descryption (Opis),
c. określenie keywords (słów kluczowych),

22) funkcjonalność konfiguracji kont email przeznaczonych do obsługi np. formularza kontaktowego, newslettera,

23) funkcjonalność tworzenia, udostępnienia i zarządzania deklaracją dostępności zgodnej ze wzorem opublikowanym przez właściwego Ministra, zgodnie z wymogami Ustawy o dostępności cyfrowej z dnia 4 kwietnia 2019 roku.

4. Pozostałe wymagania dla usługi chmurowej - serwisu www.

1) Wykonany serwis www powinien spełniać wymagania obowiązujących przepisów prawa.

2) Serwis internetowy musi być przygotowany w wersji responsywnej (automatyczne dopasowującej się rozdzielczości urządzeń na których jest przeglądana, a także do różnych przeglądarek internetowych).

3) Serwis internetowy musi być przygotowany w technologii umożliwiającej korzystanie ze strony internetowej na urządzeniach mobilnych w podobny sposób, jak działa mobilna aplikacja natywna. Serwis www musi posiadać możliwość „zainstalowania" na urządzeniach mobilnych poprzez dodanie ikonki na ekran urządzenia mobilnego, po tej czynności w celu przeglądania treści serwisu, wystarczy kliknąć na ikonkę strony www, a strona będzie działała jak mobilna aplikacja mobilna- treści powinny być częściowo dostępne nawet, bez połączenia z Internetem- technologia Progressive Web Apps (PWA) lub równoważna.

4) Technologia wykonania powinna pozwalać na rozbudowę serwisu www oraz na podłączenie dodatkowych funkcjonalności w przyszłości.

5) Zarówno serwis www, jak i system CMS powinny być obsługiwane przez najpopularniejsze i najbardziej aktualne przeglądarki: IE, Mozilla Firefox, Google Chrome, Opera.
6) Wymagane jest zastosowanie technologii PHP, AJAX, PWA bądź innych technologii o porównywalnych możliwościach.
7) Narzędzia do obsługi serwisu www muszą spełniać zalecenia ATAG i być dostępne dla użytkowników niepełnosprawnych, a w szczególności:
    a. Serwis internetowy powinien dać się obsłużyć przy użyciu klawiatury.
    b. Serwis internetowy nie może być zbudowany na bazie tabel, traktowanych jako element konstrukcji layoutu.
    c. Wszystkie elementy graficzne muszą mieć możliwość ustawienia tekstu alternatywnego przez redaktora.
    d. Serwis internetowy powinien oferować dostęp do wszystkich informacji przy wyłączonej obsłudze Java Script.
    e. Wszystkie formularze w serwisie muszą być zgodne ze standardami i przetestowane pod kątem dostępności dla osób niepełnosprawnych.
8) Każdy widok serwisu www musi mieć przez cały czas widoczny link/element graficzny umożliwiający powrót do strony głównej.
9) Zamawiający dopuszcza ze względów bezpieczeństwa danych tylko dedykowane dla jednostek administracji publicznej, autorskie rozwiązanie CMS, czyli CMS nie może być oparty o rozwiązanie Open Source.

Usługa chmurowa - strona Biuletynu Informacji Publicznej. Usługa ma być świadczona wraz z aktualizacją i opieką autorską w formie gwarancji na okres minimum 60 miesięcy

1. **Wdrożenie i świadczenie usługi Biuletynu Informacji Publicznej w oparciu o szablon graficzny (w tym w wersji podstawowej i w odcieniach szarości – możliwy np. do zastosowania w przypadku żałoby), który będzie zawierał min. następujące funkcjonalności:**
    1) ogłoszenia,
    2) system banerowy,
    3) pop up,
    4) mapa serwisu odzwierciedlającą widoczne elementy struktury serwisu,
    5) powiadomienia Web Push,
    6) statystyki odwiedzin zintegrowane z Google Analytics,
    7) funkcja strony do druku dla każdej informacji tekstowej, dostępna poprzez ikonkę pod każdą informacją,
    8) wyszukiwarka,
    9) formularz kontaktowy,
    10) możliwość „zainstalowania" serwisu www na urządzeniach mobilnych poprzez dodanie ikonki na ekran urządzenia mobilnego, po tej czynności w celu przeglądania treści serwisu, wystarczy kliknąć na ikonkę strony www, a strona będzie działała jak mobilna aplikacja natywna- treści powinny być częściowo dostępne nawet, bez połączenia z Internetem;
    11) rejestr/dziennik zmian,
    12) redakcja BIP,
    13) wersja BIP o wysokim kontraście,
    14) powiększanie/pomniejszenie czcionki,

15) link graficzny do strony głównej BIP.GOV.PL,
16) instrukcja obsługi,
17) deklaracja dostępności,

2. **Wymagania dotyczące systemu CMS do zarządzania usługą chmurową - stroną Biuletynu Informacji Publicznej dostępne w panelu zarządzania:**
   1) panel administracyjny w polskiej wersji językowej,
   2) system CMS musi posiadać mechanizm przekierowujący użytkownika na zaprojektowaną przez Wykonawcę stronę informacji o błędzie (ERROR 404) w przypadku podania niewłaściwego adresu strony WWW, na której znajdzie się informacja o braku szukanego adresu oraz link do strony głównej danej strony WWW,
   3) system CMS musi dawać informację o miejscu w strukturze serwisu internetowego, w którym znajduje się aktualnie użytkownik,
   4) dostęp do panelu administracyjnego powinien być możliwy poprzez wejście na konkretny adres strony www, szyfrowany za pomocą certyfikatu SSL, za pomocą loginu i hasła,
   5) system CMS dostarczony przez Wykonawcę musi umożliwiać zarządzanie treścią całego serwisu internetowego bez konieczności znajomości języków programowania (do obsługi ma być wystarczająca podstawowa znajomość programów do edycji tekstu).
   6) system CMS musi obsługiwać wszystkie strony serwisu internetowego BIP oraz wszystkie bazy, rejestry, listy etc.
   7) system CMS musi automatycznie oznaczać czasem, bez możliwości ingerencji, każdą wytworzoną/udostępnioną informację lub plik zgodnie z wymogami prawa,
   8) system CMS musi częściowo automatycznie tworzyć dla każdej udostępnionej informacji, pliku tzw. metryczkę zawierającą datę wytworzenia, osobę wytwarzającą informację/plik, datę publikacji, osobę publikującą, datę ostatniej modyfikacji, osobę modyfikującą,
   9) system CMS musi posiadać funkcjonalność tworzenia i zarządzania różnego rodzaju rejestrami np. rejestr zamówień publicznych, oświadczeń majątkowych, zarządzeń itp. z możliwością:
      a) tworzenia do 6 poziomów struktury rejestru,
      b) możliwość dodawania do elementu rejestru treści (wysiwyg) oraz załączników,
      c) możliwość zmiany kolejności wyświetlania,
      d) możliwość zmiany widoczności elementów rejestru,
   10) system CMS musi automatycznie tworzyć dziennik zdarzeń, zawierający zgodnie z obowiązującymi przepisami prawa, wszelkie operacje dotyczące udostępnionych informacji i plików, logowań do panelu administracyjnego, w tym przede wszystkim prezentuje:
      a) dokładny czas operacji,
      b) nazwa elementu struktury/nazwa pliku,
      c) rodzaj operacji,
      d) redaktor
   11) pełne zarządzanie menu, tzn. dodawanie/usuwanie zakładek i podzakładek; możliwość stworzenia minimum 3 poziomów struktury menu,
   12) tworzenie linków między zakładkami i podzakładkami,
   13) budowanie hierarchii menu, w tym struktury, która pozostaje nie widoczna na stronie prezentacyjnej,
   14) możliwość zmiany umiejscowienia elementów struktury menu, w tym kolejności wyświetlania oraz przenoszenia poszczególnych elementów np. zakładki do innego działu, podzakładki do innej zakładki,

15) możliwość zmiany poziomu elementu struktury (np. zmiana zakładki na podzakładek) – wszystko poprzez wybór w edycji danego elementu, miejsca docelowego z dostępnej struktury,
16) zarządzanie widocznością i publikacją elementów struktury,
17) możliwość podejrzenia tworzonej treści bez jej publikacji na stronie wynikowej,
18) możliwość włączenia i wyłączenia graficznej wersji żałobnej serwisu,
19) łatwa, pełna edycja tekstu za pomocą WYSIWYG, w tym z możliwością:
    a. pogrubienia, kursywy, podkreślenia tekstu,
    b. wyrównania tekstu, zdjęcia, tabelki: do lewej, do środka, do prawej, równaj do prawej i lewej,
    c. skorzystania z wbudowanych styli: nagłówki od 1 do 6
    d. skorzystania z listy wbudowanych rodzajów czcionek,
    e. określenia wielkości czcionki w danym tekście,
    f. określenia koloru czcionki oraz koloru tła pod tekstem,
    g. kopiowania, wycinania i wklejania podczas edycji treści,
    h. wklejania treści z edytorów tekstu np. z MS Word,
    i. zastosowania listy numerowanej i punktowanej,
    j. zastosowania wcięcia, cofnięcia wcięcia,
    k. cofnięcia i ponowienia operacji,
    l. wstawienia i edytowania linków do: pliku, zdjęcia, adresu email, strony www – z określeniem czy w tym samym oknie, czy w nowym,
    m. wstawienia pliku graficznego w treści za pomocą przeglądaj dysk, z możliwością
        i. określenia tytułu pliku oraz opisu alternatywnego,
        ii. określenia pozycji zdjęcia względem tekstu (wyrównanie do lewej lub prawej, oblanie tekstem, pozycja zdjęcia względem tekstu)
        iii. wstawienie ramki z określeniem jej grubości,
    n. przełączenia się w tryb HTML,
    o. wstawienia filmu lub pliku audio,
    p. wstawienia tabeli z możliwością:
        i. ustawienia liczby kolumn i wierszy
        ii. określenia odległości komórek od siebie,
        iii. określenia zawartości komórki od jej ramki,
        iv. wyrównanie tabeli względem tekstu,
        v. określenie obramowania tabeli,
        vi. szerokości i wysokości
        vii. kolor ramki i kolor tła,
20) dodawanie plików graficznych i multimedialnych, do każdej podstrony tekstowej struktury serwisu,
21) każdy plik graficzny musi posiadać możliwość przy jego dodawaniu, określenia jego tytułu, opisu alternatywnego,
22) funkcjonalność umożliwiająca zarządzanie ogłoszeniami:
    a. zarządzanie aktualnością – dodawanie nowej, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
    b. załączanie plików, w tym:
        i. plików graficznych, które muszą posiadać możliwość kadrowania, obracania, powiększania i pomniejszania – w celu uzyskania odpowiedniej kompozycji,

ii. załączane pozostałe pliki jako załączniki – muszą być prezentowany w sposób automatyczny na stronie wynikowej (bez potrzeby ingerencji osoby redagującej), zgodnie z wymogami WCAG 2.1

23) funkcjonalność umożliwiająca zrządzanie banerami:
    a. zarządzanie banerami - dodawanie nowego, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności,
    b. tworzenie pop-up na warstwie,
    c. możliwość linkowania do stron zewnętrznych oraz podstron serwisu,
24) funkcjonalność zarządzania użytkownikami systemu:
    a. lista użytkowników,
    b. dodawanie i zarządzanie użytkownikami,
    c. nadawanie uprawnień do poszczególnych modułów oraz funkcjonalności dla utworzonych grup,
    d. możliwość tworzenia i zarządzania grupami użytkowników np. administratorzy, redaktorzy – wraz z przydzieleniem ich dostępu do określonych modułów, funkcjonalności,
    e. możliwość odblokowywania zablokowanych użytkowników z powodu błędnego logowania,
25) funkcjonalność integracji z kontem Google Analytics w celu uzyskania szczegółowych statystyk odwiedzin serwisu.
26) funkcjonalność SEO – w celu określenia podstawowych danych serwisu, podlegających indeksowaniu przez wyszukiwarki internetowe, umożliwiająca co najmniej:
    a. określenie pola Title (tytuł),
    b. określenie pola Descryption (Opis),
    c. określenie keywords (słów kluczowych),
27) funkcjonalność konfiguracji kont email przeznaczonych do obsługi np. formularza kontaktowego,
28) funkcjonalność tworzenia, udostępnienia i zarządzania deklaracją dostępności zgodnej ze wzorem opublikowanym przez właściwego Ministra, zgodnie z wymogami Ustawy o dostępności cyfrowej z dnia 4 kwietnia 2019 roku.
29) Funkcjonalność dodawania załączników do każdej strony i podstrony w strukturze BIP zgodnie z wymogami WCAG 2.1

3. Pozostałe wymagania dla Biuletynu Informacji Publicznej.

1) Wykonany serwis BIP musi spełniać wymagania obowiązujących przepisów prawa w tym w szczególności zawarte w :
    a. Ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej,
    b. Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych,
    c. Ustawie z dnia 16 września 2011 r. o zmianie ustawy o dostępie do informacji publicznej wdraża dyrektywę unijną 2003/98/WE Parlamentu Europejskiego.
    d. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r.w sprawie Biuletynu Informacji Publicznej,
    e. Rozporządzeniu Rady Ministrów z dnia 12 marca 2014 r. w sprawie Centralnego Repozytorium Informacji Publicznej,
    f. Rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności z 12.04.2012 r. oraz wymagania WCAG 2.1 (Web Content Accessibility Guidelines) dla systemów teleinformatycznych w zakresie dostępności dla osób niepełnosprawnych, zgodnie z zapisami Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych,

g. Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE 4.5.2016);
h. Dyrektywie (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz. Urz. UE 2.12.2016);
i. Ustawie o ponownym wykorzystywaniu informacji sektora publicznego z dnia 25 lutego 2016 r. (Dz.U. z 2016 r. poz. 352);
j. Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 poz. 1219, z późn. zm.).
k. Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570, z późn. zm.) oraz jej aktami wykonawczymi, w szczególności z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247), w tym z załącznikiem nr 4 do rozporządzenia w sprawie wytycznych WCAG 2.0 (System CMS musi zapewniać ich walidację);
l. Ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2019 poz. 848);
m. Ustawie z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907, z późn. zm.), w szczególności z art. 173 ustawy;

2) Serwis internetowy BIP musi być przygotowany w wersji responsywnej (automatyczne dopasowującej się rozdzielczości urządzeń na których jest przeglądana, a także do różnych przeglądarek internetowych).
3) Serwis internetowy BIP musi być przygotowany w technologii umożliwiającej korzystanie ze strony internetowej na urządzeniach mobilnych w takim sam sposób, jak w mobilnej aplikacji natywnej.
4) Technologia wykonania strony BIP powinna pozwalać na rozbudowę strony oraz na podłączenie do niej dodatkowych funkcjonalności w przyszłości.
5) Zarówno strona jak i system CMS powinny być obsługiwane przez najpopularniejsze przeglądarki: IE, Mozilla Firefox, Google Chrome, Opera.
6) Wymagane jest zastosowanie technologii PHP lub JAVA oraz AJAX (szczególnie do funkcjonalności: galeria zdjęć, kalendarz, wyszukiwarka) bądź innych technologii o porównywalnych możliwościach.
7) Narzędzia do obsługi serwisu BIP muszą spełniać zalecenia ATAG i być dostępne dla użytkowników niepełnosprawnych, a w szczególności:
    a. Serwis internetowy BIP powinien dać się obsłużyć przy użyciu klawiatury.
    b. Serwis internetowy BIP nie może być zbudowany na bazie tabel, traktowanych jako element konstrukcji layoutu.
    c. Wszystkie elementy graficzne muszą mieć zrozumiały tekst alternatywny lub możliwość ustawienia takiego tekstu przez redaktora.
    d. Serwis internetowy BIP powinien oferować dostęp do wszystkich informacji przy wyłączonej obsłudze Java Script.
    e. Wszystkie formularze w serwisie muszą być zgodne ze standardami i przetestowane pod kątem dostępności dla osób niepełnosprawnych.

8) Każdy layout strony musi mieć przez cały czas widoczny link umożliwiający powrót do strony głównej z każdego miejsca na stronie WWW i odsyłacz umożliwiający powrót na początek strony.
9) Zamawiający dopuszcza ze względów bezpieczeństwa danych tylko dedykowane dla jednostek administracji publicznej, autorskie rozwiązanie CMS.