Załącznik nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup licencji systemu e-Urząd

w ramach projektu

„Elektroniczna administracja w Powiecie Proszowickim”

Projekt finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego (EFRR) w ramach Regionalnego Programu Operacyjnego Województwa Małopolskiego na lata 2014 – 2020, II Osi Priorytetowej „CYFROWA MAŁOPOLSKA”, Działanie 2.1 „E-administracja i otwarte zasoby”.

Spis treści

I. KONCEPCJA SYSTEMU 3
II. ZAKRES DOSTAW I USŁUG 4
III. SYSTEMY UŻYWANE W URZĘDZIE 5
IV. DOSTĘPNA INFRASTRUKTURA SPRZĘTOWA 5
V. RÓWNOWAŻNOŚĆ ROZWIĄZAŃ 6
VI. MINIMALNE WYMAGANIA 7
CZĘŚĆ I - PORTAL E-USŁUG 7
CZĘŚĆ II – ROZWIĄZANIA BEZPIECZEŃSTWA 21

I. KONCEPCJA SYSTEMU

Celem projektu **„Elektroniczna administracja w Powiecie Proszowickim”** jest wsparcie rozwoju elektronicznych usług publicznych w zakresie e-administracji oraz zwiększenie dostępu zarówno obywateli jak i przedsiębiorców do cyfrowych usług publicznych on-line.

Centrum elektronicznych usług publicznych będzie stanowił dedykowany portal usług publicznych dla klientów urzędu, którymi mogą być zarówno mieszkańcy, przedsiębiorcy czy konkretnie podatnicy lub inwestorzy. Oferowane w ramach portalu usługi będą równoważne co do wykonywanych usług w standardowym trybie, jednakże cały proces będzie się odbywał automatycznie z wykorzystaniem rozwiązań informatycznych bez konieczności wizyty klienta w siedzibie Urzędu. E-Usługi mają też być dostępne na urządzeniach mobilnych.

Portal będący centrum usług publicznych będzie udostępniał następujące grupy usług:

- informacje publiczne;
- informacje spersonalizowane przeznaczone dla konkretnych podmiotów i obywateli udostępniane po uwierzytelnieniu.

Elektroniczne usługi uruchomione w ramach projektu muszą zapewnić całą i kompletną ścieżkę realizacji danej sprawy. Usługi muszą być zainicjowane (o ile istnieje taka potrzeba) przesłaniem za pomocą platformy ePUAP dokumentu elektronicznego na skrzynkę podawczą urzędu. Następnie dokument musi być elektronicznie przekazany do osób merytorycznie odpowiedzialnych za procedowanie sprawy. Po zatwierdzeniu wniosku zostanie naliczona odpowiednia opłata. Po wygenerowaniu wysokości zobowiązania, interesant może zostać powiadomiony o tym fakcie poprzez e-mail, sms lub wiadomością na platformę ePUAP. W ramach portalu usług publicznych może on zobaczyć wysokość swojego zobowiązania, dane dodatkowe, terminy płatności oraz uiścić opłatę wraz z wyborem konkretnych zobowiązań i rat tych zobowiązań. Płatności zostają zaksięgowane w systemach dziedzinowych wewnątrz urzędu co jest widoczne także w niniejszym portalu. Po zakończeniu całości płatności klient może zostać o tym fakcie powiadomiony za pomocą sms, e-mail lub przez platformę ePUAP. Za pomocą tych samych kanałów informacyjnych, klient zostanie powiadomiony o fakcie wydania decyzji.

Wynikiem realizacji zadania będzie udostępnienie 10 usług o udowodnionym poziomie dojrzałości minimum 4 (transakcja) oraz 11 usług na poziomie dojrzałości 3 (dwustronna interakcja).

Nazwa e-usługi	Poziom dojrzałości
Wydanie decyzji o pozwoleniu na budowę	4
Wydanie zaświadczenia o samodzielności lokalu	4
Wydanie zaświadczenia o braku sprzeciwu do przyjętych zgłoszeń budowlanych	4
Wydawanie kart wędkarskich	4
Wydanie kart parkingowych	4
Wydawanie i zmiana zaświadczeń na przewozy drogowe na potrzeby własne	4
Wydawanie zezwoleń kat I na przejazd pojazdu nienormatywnego	4
Wydawanie zezwoleń kat. II i III na przejazd pojazdu nienormatywnego	4
Wniosek o zajęcie pasa drogowego	4
Wydanie zaświadczenia potwierdzającego, że działka nie jest objęta uproszczonym planem urządzenia lasu lub decyzją, o której mowa w 3 art. 19 ust. 3 ustawy o lasach	4
Możliwość wypełnienia i wysłania formularza wniosku o założenie konta w Powiatowym Portalu Usług Publicznych dla osób prawnych/fizycznych	3

Możliwość wypełnienia i wysłania formularza wniosku o dezaktywację konta w Powiatowym Portalu Usług Publicznych dla osób prawnych/fizycznych	3
Możliwość wypełnienia i wysłania formularza wniosku zgłoszenia budowy lub wykonania robót budowlanych niewymagających pozwolenia na budowę	3
Możliwość wypełnienia i wysłania formularza wniosku o udzielenie informacji publicznej	3
Możliwość wypełnienia i wysłania formularza wniosku o wyłączenie gruntów rolnych z produkcji rolniczej	3
Możliwość wypełnienia i wysłania formularza zgłoszenia rozbiórki obiektu budowlanego	3
Możliwość wypełnienia i wysłania formularza wniosku o uzgodnienie warunkach zabudowy	3
Możliwość wypełnienia i wysłania formularza wniosku o wydanie legitymacji upoważniającej do zniżek na komunikację publiczną	3
Możliwość wypełnienia i wysłania formularza wniosku o usunięcie drzew i krzewów z gruntów będących własnością gminy	3
Możliwość wypełnienia i wysłania formularza wniosku o zatwierdzanie projektów zmian organizacji ruchu	3
Możliwość wypełnienia i wysłania formularza wniosku o nieodpłatną pomoc prawną	3

II. ZAKRES DOSTAW I USŁUG

Realizacja zadania służącego wdrożeniu standardów funkcjonowania cyfrowego urzędu ukierunkowana na poprawę usług publicznych przez rozwój infrastruktury e-usług oraz komunikacji elektronicznej na terenie powiatu, związanego ze świadczeniem elektronicznych usług publicznych przez Zamawiającego będzie wymagała poprawy, rozbudowy i modernizacji systemów informatycznych w zakresie:

a) wdrożenie aplikacji dziedzinowych e-Urzędu umożliwiających świadczenie e-usług na wysokim poziomie dojrzałości w zakresie udostępniania informacji i regulacji zobowiązań drogą elektroniczną wraz z wykorzystaniem platformy ePUAP w celu udostępniania e-usług publicznych;

b) wdrożenie aplikacji dziedzinowych e-Urzędu umożliwiających świadczenie e-Usług w zakresie składania elektronicznych formularzy oraz dostępu do informacji o stanie sprawy i korespondencji obejmujące opracowanie formularzy na ePUAP zintegrowanych z portalem e- Urząd;

a) wdrożenie Elektronicznego Obiegu Dokumentów w Jednostkach Organizacyjnych umożliwiając wymianę dokumentów pomiędzy Urzędem a Jednostkami Organizacyjnymi i jednoczesne uproszczenie wewnętrznych procedur co pozytywnie wpłynie na ograniczenie czasu obsługi interesantów, optymalnego wykorzystania współpracujących ze sobą urządzeń informatycznych i oprogramowania;

c) wdrożenie rozwiązań bezpieczeństwa typu DLP, pozwalających na kontrolę treści dokumentów elektronicznych i ochronę przed wyciekiem i utratą danych wrażliwych;

d) wdrożenie rozwiązań bezpieczeństwa w zakresie wykrywania luk i podatności w oprogramowaniu wykorzystywanym w sieci.

Niniejsze zamówienie zostało podzielone na części i dotyczy w szczególności dostaw i usług zgodnie z poniższym zestawieniem. Oferowane rozwiązania i usługi muszą być zgodne z minimalnymi wymaganiami zawartymi w niniejszej specyfikacji:

LP.	NAZWA URZĄDZENIA / USŁUGI	ILOŚĆ	JEDN.
CZĘŚĆ I – PORTAL E-USŁUG			
1.	Portal mieszkańca	1	kpl.
2.	System Obiegu Dokumentów dla Jednostek organizacyjnych	1	kpl.

3.	Szkolenie w zakresie e-Usług	1	kpl.
CZĘŚĆ II – ROZWIĄZANIA BEZPIECZEŃSTWA			
4.	System badania podatności	1	kpl.
5.	System DLP	1	kpl.

III. SYSTEMY UŻYWANE W URZĘDZIE

Nowe moduły oprogramowania do świadczenia e-usług będą korzystały z zasobów istniejących rozwiązań, zgodnie z poniższym zestawieniem.

PODUCENT	NAZWA SYSTEMU / RODZAJ SYSTEMU
COGISOFT	System ERP
MADKOM	Sidas EZD / elektroniczny obieg dokumentów
GEOMATYKA	EWID / system geodezyjny

IV. DOSTĘPNA INFRASTRUKTURA SPRZĘTOWA

Wszystkie dostarczone rozwiązania w ramach projektu będą instalowane na infrastrukturze sprzętowej udostępnionej przez Zamawiającego, w skład której wchodzi:

a) **Serwer baz danych** – dwa procesory wielordzeniowe, osiągające w teście PassMark CPU Mark wynik min. 20.000 punktów według wyników ze strony http://www.cpubenchmark.net/cpu_list.php dla konfiguracji dwuprocesorowej, pamięć RAM minimum 64 GB, pamięć masowa 2x600GB 10kRPM, zainstalowany system operacyjny umożliwiający uruchomienie minimum dwóch wirtualnych środowisk systemu operacyjnego;
b) **Serwer aplikacji** – dwa procesory wielordzeniowe, osiągające w teście PassMark CPU Mark wynik min. 20.000 punktów według wyników ze strony http://www.cpubenchmark.net/cpu_list.php dla konfiguracji dwuprocesorowej, pamięć RAM minimum 64 GB, HDD 2x600GB 10kRPM, zainstalowany system operacyjny umożliwiający uruchomienie minimum dwóch wirtualnych środowisk systemu operacyjnego;
c) **Macierz dyskowa** – 2 kontrolery active/actiwe RAID 1,5,6,10,50, dostępna przestrzeń dyskowa minimum netto 6TB w oparciu o RAID5;

Wykonawca zobowiązany jest zainstalować, skonfigurować i uruchomić dostarczone przez siebie rozwiązania w w/w środowisku teleinformatycznym Zamawiającego.

W przypadku, gdy Wykonawca uzna, że z jakichkolwiek względów (funkcjonalnych, wydajnościowych, bezpieczeństwa, itd.) nie jest w stanie zapewnić poprawności działania dostarczanych przez siebie rozwiązań na w/w infrastrukturze teleinformatycznej, może w takim przypadku dostarczyć dedykowaną infrastrukturę techniczną (dedykowany serwer fizyczny). W takim przypadku Wykonawca przedłoży Zamawiającemu szczegółową specyfikację sprzętu wraz z uzasadnieniem konieczności jego wdrożenia. Wykonawca może wdrożyć dodatkową infrastrukturę techniczną tylko za zgodą Zamawiającego. Wykonawca dostarcza infrastrukturę techniczną bez dodatkowego wynagrodzenia ze strony Zamawiającego, a sam sprzęt przechodzi na własność Zamawiającego. Dostarczony przez Wykonawcę sprzęt objęty jest warunkami gwarancji analogicznymi jak całość przedmiotu umowy.

Ze względu na konieczność zachowania kompatybilności z istniejącą infrastrukturą teleinformatyczną Zamawiającego, wymagane jest dostarczenie urządzeń możliwych do montaży w szafie typu RACK, wyposażonymi w zasilacze redundantne o mocy każdy o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia wraz z kablami zasilającymi, dyski twarde typu Hot-Plug w układzie RAID na poziomie 5 lub 10, karta sieciowa z czterema interfejsami sieciowymi 1Gb Ethernet w standardzie BaseT. Dostarczony sprzęt musi być objęty 5-cio letnią gwarancją producenta z serwisem realizowanym w miejscu instalacji oraz musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.

W przypadku, gdy Wykonawca uzna, że dla potrzeb instalacji dostarczonych przez siebie rozwiązań informatycznych, wymagana będzie instalacja środowisk informatycznych wykraczająca poza udostępniane przez Zamawiającego, musi dostarczyć wymagane dla rozwiązań środowiska we własnym zakresie bez dodatkowego wynagrodzenia.

V. RÓWNOWAŻNOŚĆ ROZWIĄZAŃ

W celu zachowania reguły konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych w treści niniejszego OPZ, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności przez to rozwiązanie oferowanych, 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 nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane.

Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, iż 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 (kompletne i spójne) dane, przeszkolić użytkowników, skonfigurować Oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania Oprogramowania w środowisku produkcyjnym itp. Wymiana oprogramowania musi odbywać się przy zachowaniu zasady pełnej dostępności do danych zgromadzonych w bazach informacyjnych, zgromadzonych w wyniku stosowania obecnie funkcjonujących aplikacji. Nowy system musi zapewniać ciągłość pracy pracowników i wykonywania bieżących czynności Zamawiającego bez potrzeby ręcznego uzupełniania danych.

VI. MINIMALNE WYMAGANIA

CZĘŚĆ I - PORTAL E-USŁUG

WYMAGANIA OGÓLNE

W ramach zadania, Zamawiający wymaga dostarczenia gotowego oprogramowania wraz z niezbędnymi licencjami oraz usługami wdrożeniowymi obejmującymi minimum:

- przygotowanie serwerów udostępnionych przez Zamawiającego;
- na serwerze bazodanowym - instalację i konfigurację systemu operacyjnego i motoru baz danych wymaganego dla dostarczonych rozwiązań;
- instalację i konfigurację dodatkowych usług niezbędnych do prawidłowego działania systemu zintegrowanego (jeżeli wymagane);
- na serwerze aplikacyjnym - instalację i konfigurację środowiska podstawowego zgodnie z wymaganiami instalowanego oprogramowania oraz oprogramowania e-Usług; zainstaluje dostarczy licencje na wszystkie moduły oprogramowania nie ograniczonych co do ilości użytkowników oraz nie ograniczonych czasowo;
- zabezpieczenie certyfikatem SSL, udostępnionym przez Zamawiającego, połączenia z portalem dla użytkowników zewnętrznych;
- instalację i konfigurację elektronicznych usług publicznych na serwerach;
- instalację i konfiguracje systemu elektronicznego obiegu dokumentów.

Wyłoniony dostawca oprogramowania musi udostępnić jednolity system zgłoszeń, który ma służyć do dwustronnej komunikacji, monitorowania postępu realizacji projektu.

Kluczowi użytkownicy mają mieć możliwość zgłaszania wszelkich uwag do wdrożonych systemów i portalu, w tym związanych z awariami oraz usterkami i błędami.

Wszyscy użytkownicy w ramach danej organizacji mają mieć wgląd do takich informacji jak: termin realizacji sprawy, osoba odpowiedzialna, na jakim etapie jest sprawa, opis rozwiązana danego zgłoszenia i całość historii zdarzeń.

WYMAGANIA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

W zakresie bezpieczeństwa teleinformatycznego należy uwzględnić zapisy ustawowe regulujące obowiązki przetwarzającego dane, sposoby przetwarzania i ochrony czy też sposoby testowania i odbierania systemów teleinformatycznych. W tym zakresie do najważniejszych należą:

- Ustawa o ochronie danych osobowych.
- Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.
- Ustawa o podpisie elektronicznym.
- Ustawa o świadczeniu usług droga elektroniczną.
- Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne.
- Ustawa o prawie autorskim i prawach pokrewnych.
- Ustawa o ochronie baz danych.
- Kodeks karny.
- Ustawa o ochronie informacji niejawnych.

- Ustawa o dostępnie do informacji publicznej.
- Ustawa o ochronie danych osobowych z dnia 10 maja 2018 (Dz.U. 2018 poz.1000 z późn. zm.)
- Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania
- Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
- Rozporządzenie Rady Ministrów z dnia 27 września 2005r. sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 grudnia 2011 r. w sprawie wymagań technicznych dokumentów elektronicznych zawierających akty normatywne i inne akty prawne, elektronicznej formy dzienników urzędowych oraz środków komunikacji elektronicznej i informatycznych nośników danych.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Dostarczone rozwiązanie musi:

- mieć możliwość wymiany danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących;
- w wysyłanych dokumentach w drodze teletransmisji mieć możliwość wymiany znaków wg standardu Unicode UTF-8;
- umożliwiać udostępnienie zasobów informacyjnych co najmniej w jednym z formatów wymienionych w Załączniku nr 2 do Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r.;
- mieć dostosowany portal prezentujący dane dla interesantów zgodnie z wymaganiami WCAG 2.1 w zakresie zgodnym z ww. rozporządzeniem;
- mieć możliwość tworzenia tzw. logów czyli zapisów w dziennikach systemu informacji pozwalających na m.in. rozliczalność i autentyczność informacji.

W zakresie portalu elektronicznych usług publicznych dla użytkowników zewnętrznych połączenie z portalem przez użytkowników musi być zabezpieczone certyfikatem SSL. Użytkownik zewnętrzny posiadający konto na platformie musi mieć dostęp do danych, tylko dla podmiotów do których ma przydzielone uprawnienia (na podstawie wniosku o udostępnienie konta na portalu). Dane dla portalu użytkowników zewnętrznych są replikowane (kopiowane) z systemów dziedzinowych tylko dla użytkowników, którzy złożyli wniosek o udostępnienie danych na portalu, tym samym portal nie ma bezpośredniego dostępu do baz danych systemów dziedzinowych.

WYMAGANIA FORMALNO-PRAWNE SYSTEMU E-URZĄD

System e-Urząd musi być zgodny z obowiązującym stanem prawnym we wszystkich dziedzinach funkcjonowania obsługiwanej przez system jednostki publicznej, w szczególności spełniać wszelkie wymagania stawiane normami z zakresu finansów publicznych. System zapewniać ma przestrzeganie procedur kontroli finansowej, zgodnie z obowiązującymi standardami w tym zakresie. Podstawowymi aktami prawnymi, które regulują kwestie prawne związane merytorycznie z wymaganym oprogramowaniem, są:

- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2019 poz.700), szczególnie w zakresie zgodności systemów teleinformatycznych

z minimalnymi wymaganiami dla systemów teleinformatycznych oraz obowiązkami Podmiotu Publicznego realizującego zadania publiczne, przy wykorzystaniu systemu teleinformatycznego lub z użyciem komunikacji elektronicznej,

- Ustawa z dnia 10 stycznia 2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2014 poz. 183 z późn. zm);
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2019, poz.123 z późn.zm),
- Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U.2015, poz.1341),
- Ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2019, poz.1429),
- Ustawa z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznejoraz niektórych innych ustaw (Dz.U. 2018 poz.1544),
- Ustawa z dnia 4 kwietnia 2019 roku o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2019 r. poz. 848).
- Ustawa z dnia 16 września 2011 r. o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw (Dz.U.2011.204.1195) wdrażająca Dyrektywę Parlamentu Europejskiego i Rady nr 2003/98/WE z dnia 17 listopada 2003 r. „Re-use of PSI" w sprawie ponownego wykorzystywania informacji sektora publicznego.
- Rozporządzenie 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 (Dz.U.2017, poz.2247 z poźn. zm.);
- Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz.U. 2018 poz. 29, z późn. zm);
- Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania – (Dz.U. 2005 poz. 1836);
- Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U.2018, poz. 180 z późn.zm.);

WYMAGANIA GWARANCYJNE

Wykonawca odpowiedzialny będzie za całokształt, w tym za przebieg oraz terminowe wykonanie zamówienia w okresie wykonania umowy, jak i w okresie trwania gwarancji.

Wykonawca udziela bezpłatnej gwarancji jakości/rękojmi za wady wraz z serwisem gwarancyjnym na system e-Urząd przez **okres minimum 60 miesięcy** liczonego od daty zakończenia wdrożenia potwierdzonego protokołem odbioru końcowego, obejmującej:

- czas reakcji serwisu na błąd krytyczny nieprzekraczający 12 godzin roboczych od momentu skutecznego zgłoszenia awarii rozwiązań (drogą telefoniczną, mailową lub poprzez portal serwisowy) do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego błędu;
- czas reakcji serwisu na usterkę nieprzekraczający 24 godziny robocze od momentu skutecznego zgłoszenia usterki rozwiązań (drogą telefoniczną, mailową lub poprzez portal serwisowy) do chwili podjęcia przez Wykonawcę czynności zmierzających do usunięcia zgłoszonej usterki;
- czas usunięcia błędu krytycznego nieprzekraczający 24 godziny robocze od momentu podjęcia czynności serwisowych;
- czas usunięcia usterki nieprzekraczający 7 dni roboczych od momentu podjęcia czynności serwisowych.

Gwarancja jakości obejmuje utrzymanie systemu w ruchu oraz dostarczanie i implementację nowszych wersji oprogramowania w przypadku dostosowania go przez wykonawcę do nowych przepisów prawa.

Serwis gwarancyjny obejmuje wszelkie usługi zapewniające prawidłowe działanie systemu informatycznego, tj. usuwanie awarii i usterek, instalowanie poprawek (patch), instalowanie nowych wersji oprogramowania, jeżeli jest to niezbędne w celu usunięcia awarii lub usterki, zapewnienia bezpieczeństwa danych, usunięcia błędów w działaniu wdrożonych rozwiązań, udzielanie konsultacji telefonicznych oraz odpowiedzi na zapytania przesłane za pomocą portalu zgłoszeniowego udostępnionego przez producenta.

Po usunięciu każdej awarii lub usterki, Wykonawca zobowiązuje się do doprowadzenia całego systemu informatycznego do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów.

Każda wizyta/przegląd/naprawa gwarancyjna wykonywana w miejscu instalacji systemu informatycznego będzie zakończona spisaniem właściwego protokołu.

Zamawiający zapewni serwisowi Wykonawcy dostęp do systemu informatycznego od momentu zgłoszenia przez czas potrzebny na usunięcia awarii/usterki, o ile nie będzie to zakłócało działań własnych Zamawiającego.

Gwarancją jakości są także objęte dane przetwarzane przez dostarczone rozwiązania informatyczne w zakresie poprawności i integralności danych.

Na potrzeby zapisów dotyczących gwarancji jakości i serwisu gwarancyjnego ustala się następujące definicje użytych pojęć:

USTERKA – zdarzenie, w którym uszkodzeniu uległ jeden (lub więcej) element/moduł systemu, nie wpływający/e na funkcjonalność i wydajność systemu, ale niezgodny ze stanem określonym w Opisie Przedmiotu Zamówienia oraz Zestawieniu Oferowanych Rozwiązań lub dokumentacji technicznej i instrukcji użytkownika, będących załącznikiem do Umowy

BŁĄD KRYTYCZNY – zdarzenie, w którym uszkodzeniu uległ jeden (lub więcej) element/moduł systemu, ograniczający/e wydajność lub funkcjonalność systemu i uniemożliwiający/e Zamawiającemu na korzystanie z oprogramowania zgodnie z jego dokumentacją techniczną/instrukcją użytkowania.

W okresie trwania gwarancji jakości/rękojmi za wady na przedmiot umowy wszelkie koszty usuwania wad i awarii, których przyczyna nie leży po stronie Zamawiającego ponosi Wykonawca.

1. PORTAL MIESZKAŃCA

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY FUNKCJONALNE
WYMAGANIA OGÓLNE	Dostarczane rozwiązania muszą być zgodne z obowiązującym stanem prawnym, przepisami prawnymi regulującymi działalność samorządu we wszystkich dziedzinach jego funkcjonowania. W szczególności muszą być zgodne z Krajowymi Ramami Interoperacyjności oraz jeżeli jest to wymagane dla poszczególnych systemów to muszą umożliwiać wymianę danych z innymi rejestrami publicznymi. Rozwiązania udostępnione dla interesantów muszą cechować się wysoką funkcjonalnością zaplanowanych rozwiązań. Portal musi mieć możliwość obsługi za pomocą najpopularniejszych przeglądarek internetowych (min. Edge, Chrome, Mozilla Firefox), a także za pomocą urządzeń mobilnych. Strona portalu musi być responsywna, dostosowując się do rozdzielczości urządzenia na jakim będzie oglądana.

	Zamawiający wymaga, aby portal udostępniał informacje publiczne po uwierzytelnieniu z danych strukturalnych w zakresie: - opłat z tytułu wydania decyzji o pozwoleniu na budowę wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności i przeterminowanie); - opłat z tytułu wydania zaświadczenia o samodzielności lokalu wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności, przeterminowanie i informacji o tytule płatności); - opłat z tytułu wydania zaświadczenia o braku sprzeciwu do przyjętych zgłoszeń budowlanych wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności, przeterminowanie i informacji o tytule płatności); - opłat z tytułu wydania karty wędkarskiej wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności, przeterminowanie i informacji o tytule płatności); - opłat z tytułu wydania karty parkingowej wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności, przeterminowanie i informacji o tytule płatności); - opłat z tytułu wydania i zmiany zaświadczenia na przewozy drogowe na potrzeby własne wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności, przeterminowanie i informacji o tytule płatności); - opłat z tytułu wydania zezwoleń kat I na przejazd pojazdu nienormatywnego wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności, przeterminowanie i informacji o tytule płatności); - opłat z tytułu wydania zezwoleń kat. II i III na przejazd pojazdu nienormatywnego wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności, przeterminowanie i informacji o tytule płatności); - opłat z tytułu wydania zezwoleń na zajęcie pasa drogowego wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności, przeterminowanie i informacji o tytule płatności); - opłat z tytułu zaświadczenia potwierdzającego, że działka nie jest objęta uproszczonym planem urządzenia lasu lub decyzją, o której mowa w art. 19 ust. 3 ustawy o lasach wraz z udostępnieniem informacji dotyczących: danych finansowych (globalne kwoty należności i wpłat, harmonogram płatności, realizacja płatności, przeterminowanie i informacji o tytule płatności); - zgłoszenia budowy lub wykonania robót budowlanych niewymagających pozwolenia na budowę; - udzielenia informacji publicznej; - wyłączenia gruntów rolnych z produkcji rolniczej; - zgłoszenia rozbiórki obiektu budowlanego; - uzgodnienia decyzji o warunkach zabudowy; - wydania legitymacji upoważniającej do zniżek na komunikację publiczną;

	- wydania decyzji na usuwanie drzew i krzewów z gruntów będących własnością gminy; - zatwierdzenia projektów zmian organizacji ruchu; - udzielenia nieodpłatnej pomocy prawnej. Zamawiający dopuszcza rozwiązania równoważne w zakresie Portalu Mieszkańca, pod warunkiem spełnienia wszystkich minimalnych funkcjonalności opisanych w dalszej części. Portal elektronicznych usług publicznych ma stanowić jednolitą platformę internetową pozwalającą na wymianę danych, w szczególności dokumentów, pomiędzy jednostkami samorządu terytorialnego, a obywatelami. Platforma ma posiadać wydzieloną część publiczną, w ramach której wyróżnia się obszar dostępny dla niezalogowanych i zalogowanych (po przejściu rejestracji) użytkowników/klientów systemu oraz część niepubliczną – panelem administratora służącym zarządzaniu systemem. Oba obszary muszą być dostępne z poziomu przeglądarki internetowej. Platforma w części publicznej ma udostępniać szereg narzędzi pozwalających na dwukierunkowy kontakt obywatela z urzędem. Do najważniejszych należą formularze elektroniczne pozwalające na składanie wniosków w postaci elektronicznej do jednostek samorządu terytorialnego. Platforma ma umożliwiać umieszczanie na froncie (w części publicznej) dowolnej liczby usług publicznych. Każda usługa publiczna musi się składać z opisu usługi publicznej wspólnego dla wszystkich jednostek udostępniających daną usługę publiczną oraz z tzw. karty usługi – danych dotyczących usługi specyficznych dla danego podmiotu publicznego (np. w przyszłości, gdy Gmina zdecyduje się udostępniać na portalu e-usługi jednostek organizacyjnych) . Ponadto dla tej samej usługi publicznej, podmioty muszą mieć możliwość udostępniania różnych i w różnej liczbie formularzy elektronicznych. Wspólny opis usługi publicznej musi obejmować: a. Nazwę usługi. b. Informację, kogo dotyczy usługa. c. Skrócony opis usługi. d. Informację o podstawie prawnej z możliwością wskazania wielu różnych podstaw prawnych (tj. ustawa, rozporządzenie, inne) w szczegółowości do: nazwy aktu prawnego, rocznika, adresu publikacji w dzienniku ustaw, artykułu, paragrafu, ustępu, punkty, litery i tiretu. e. Listę dokumentów wymaganych do złożenia przez interesanta dla realizacji usługi publicznej. f. Pełną informację o wszystkich opłatach w związku z realizacją usługi. g. Czasie realizacji usługi. h. Informacje o trybie odwoławczym. i. Dowolne, stałe i jednakowe dla wszystkich opisów usług, treści dodatkowe (np. tytuły, dodatkowe nagłówki, treści ogólne pomocy), które administrator ma możliwość edytować. Portal musi synchronizować treści opisów usług z systemem ePUAP za pomocą usługi sieciowej przez nią udostępnianej z częstotliwością co 24h. W ramach synchronizacji system musi także pobierać nowododane na platformie ePUAP opisy usług publicznych celem ich wykorzystania w usłudze.

	Platforma musi udostępniać słownik pozwalający na szczegółowy przegląd treści pobranych z ePUAP opisów usług. W przypadku aktualizacji opisu usługi platforma musi automatycznie zaktualizować treść usługi dostępnej publicznie.
ZARZĄDZANIE UŻYTKOWNIKAMI	Obsługa własnych kont użytkowników systemu. Zarządzanie użytkownikami Portalu: zakładanie nowych użytkowników i modyfikacja istniejących, nadawanie identyfikatora, rejestracja daty założenia, wprowadzanie i modyfikacja opisu użytkownika systemu, ustawianie i zmiana hasła, blokowanie i odblokowywanie konta użytkownika, przydzielanie uprawnień - nadawanie i odbieranie uprawnień do poszczególnych funkcji/modułów. Możliwość wykorzystania kont użytkowników z platformy ePUAP do logowania do systemu (integracja z ePUAP w zakresie „single sign-on"). Obsługa mechanizmu pełnomocnictw. Musi udostępniać narzędzia dla administratora portalu. Narzędzia będą umożliwiały zarządzanie publikowanymi dokumentami.
ZARZĄDZANIE FORMULARZAMI	Opracowanie i przygotowania następujących e-Usług na platformę ePUAP i jednocześnie na Platformę Elektronicznych Usług Publicznych (wzory formularzy w formie papierowej przekaże Zamawiający) przy czym Zamawiający wymaga automatycznej replikacji e-Usług tj. w sytuacji opublikowania jakiejkolwiek nowej e-Usługi na platformie ePUAP – taka e-Usługa ma się automatycznie pojawić na platformie elektronicznych usług publicznych Starostwa Powiatowego w Proszowicach: - Formularz ePUAP w sprawie wydania decyzji o pozwoleniu na budowę; - Formularz ePUAP w sprawie wydania zaświadczenia o samodzielności lokalu; - Formularz ePUAP w sprawie wydania zaświadczenia o braku sprzeciwu do przyjętych zgłoszeń budowlanych; - Formularz ePUAP w sprawie wydania karty wędkarskiej; - Formularz ePUAP w sprawie wydania karty parkingowej; - Formularz ePUAP w sprawie wydania i zmiany zaświadczenia na przewozy drogowe na potrzeby własne; - Formularz ePUAP w sprawie wydania zezwoleń kat I na przejazd pojazdu nienormatywnego; - Formularz ePUAP w sprawie wydania zezwoleń kat. II i III na przejazd pojazdu nienormatywnego; - Formularz ePUAP Wniosek o zajęcie pasa drogowego; - Formularz ePUAP w sprawie wydania zaświadczenia potwierdzającego, że działka nie jest objęta uproszczonym planem urządzenia lasu lub decyzją, o której mowa w art. 19 ust. 3 ustawy o lasach; - Formularz ePUAP w sprawie zgłoszenia budowy lub wykonania robót budowlanych niewymagających pozwolenia na budowę; - Formularz ePUAP w sprawie udzielenia informacji publicznej; - Formularz ePUAP w sprawie wyłączenia gruntów rolnych z produkcji rolniczej; - Formularz ePUAP w sprawie zgłoszenia rozbiórki obiektu budowlanego; - Formularz ePUAP w sprawie uzgodnienia decyzji o warunkach zabudowy; - Formularz ePUAP w sprawie wydania legitymacji upoważniającej do zniżek na komunikację publiczną; - Formularz ePUAP w sprawie wydania decyzji na usuwanie drzew i krzewów z gruntów będących własnością gminy; - Formularz ePUAP w sprawie zatwierdzenia projektów zmian organizacji ruchu;

	- Formularz ePUAP w sprawie udzielenia nieodpłatnej pomocy prawnej. Przygotowanie formularzy obejmuje: - opracowanie wzoru dokumentu elektronicznego publikowanego w CRWDE, - opracowanie formularza elektronicznego, - publikację wzoru dokumentu elektronicznego w CRWDE oraz instalację i udostępnienie elektronicznej usługi publicznej. - opracowanie kart e-usług zgodnie z obowiązującymi przepisami prawa, zawierające min. opis ogólny, wymagane dokumenty, sposób dostarczania dokumentów, sposób wykorzystania skrzynki kontaktowej i e-formularzy, opłaty, termin i sposób załatwienia sprawy, informacje na temat przebiegu sprawy, podstawę prawną. Karta usługi musi obejmować, co najmniej: a. Informację o kategorii usługi publicznej dostępnej dla celów zarządczych (kategoria widoczna tylko z poziomu panelu administracyjnego). b. Klasyfikację (bądź wiele klasyfikacji) w ramach, których usługa jest dostępna na froncie. c. Dane usługodawcy (podmiotu publicznego) tj. nazwę, komórkę organizacyjną, adres, strona BIP, telefon, fax. d. Informację o miejscu składania dokumentów – dla dokumentów w postaci innej niż elektroniczna. e. Informację o terminach przyjęć interesantów. f. Uwagi. g. Informację o usługach powiązanych. h. Zakres obszaru, dla którego dany podmiot realizuje usługę publiczną wg podziału terytorialnego kraju (TERYT). i. Dowolne, stałe i jednakowe dla wszystkich opisów usług, treści dodatkowe (np. tytuły, dodatkowe nagłówki, treści ogólne pomocy), które administrator ma możliwość edytować. Układ graficzny wszystkich formularzy musi być jednolity. W budowanych formularzach należy wykorzystać mechanizm automatycznego pobierania danych z profilu w celu uzupełnienia danych klienta. Pola PESEL, REGON lub kod pocztowy muszą być walidowane pod kątem poprawności danych wprowadzonych przez klienta. Dokumenty elektroniczne powinny być zgodne ze standardem dokumentów ePUAP. Wygenerowane dla poszczególnych formularzy wzory dokumentów elektronicznych składające się z plików: wyróżnik, schemat, wizualizacja, muszą zostać dostosowane do wymogów formatu dokumentu publikowanych w CRD i RWD oraz spełniać wymogi interoperacyjności. Formularze elektroniczne muszą być dostępne w ramach kart usług – szczegółowo opisujących usługę świadczoną w sposób elektroniczny przez podmioty publiczne. Platforma musi umożliwiać zasilenie karty usługi opisem usługi dostępnym na ePUAP. W powiązaniu z formularzami elektronicznymi musi istnieć możliwość wniesienia opłaty dotyczącej usługi za pomocą środków komunikacji elektronicznej.
WYŚWIETLANIE INFORMACJI O STANIE SPRAWY I KORESPONDENCJI	Udostępnienie po uwierzytelnieniu w portalu internetowym następujących informacji: a) stan spraw osób fizycznych i prawnych np. znak sprawy, przewidywany termin zakończenia, osoba prowadząca.

	b) informacje o korespondencji np. data wpływu, znak sprawy, nr korespondencji. Musi umożliwiać Interesantom Urzędu bieżące śledzenie stanu realizacji sprawy. Portal musi pozwalać na integrację z Systemem Elektronicznego Zarządzania Dokumentami w zakresie: a) Dwukierunkowego przekazywania dokumentów elektronicznych przy użyciu profilu interesanta. b) Wymiany informacji o statusie rozpatrywania sprawy w Systemie Elektronicznego Zarządzania Dokumentami. Przekazywania danych profilu interesanta w ramach którego został złożony wniosek w postaci dokumentu elektronicznego.
INTEGRALNOŚĆ I BEZPIECZEŃSTWO	W celu zapewnienia integralności i bezpieczeństwa danych portal musi bazować na danych zawartych w systemach dziedzinowych obecnie obsługujących wybrane obszary, w zakresie których będą prezentowane informacje.
UWIERZYTELNIANIE	Do uwierzytelniania się w portalu system musi zapewniać możliwość wykorzystania profil zaufanego, który musi być realizowany poprzez integrację z usługą oferowaną za pomocą platformy ePUAP – „Single Sign On”. Musi zapewnić kontrolę „siły” hasła, jego unikalność wstecz oraz wymuszanie zmian w określonych okresach czasu.
INNE WYMAGANIA	Portal musi być zgodny ze standardami dostępności treści internetowych na poziomie WCAG 2.1. Portal musi produkować kod HTML5 wg specyfikacji W3C http://www.w3.org/TR7html5/ Portal musi wspierać CSS 3.0 wg specyfikacji http://www.w3.org/TR/CSS/ Portal musi spełniać postulaty accessibility wg http://www.w3.org/standards/webdesign/accessibility Dostęp za pomocą przeglądarki internetowej. Możliwość realizacji płatności należności podatkowych poprzez usługę wybranego operatora płatności elektronicznych. Zgodnie w wytycznymi UODO, musi istnieć możliwość rejestrowania zdarzeń polegających na przeglądaniu danych - kto i kiedy korzystał z danej Bazy które rekordy były odczytywane. Dostarczony portal musi mieć możliwość obsługi za pomocą najpopularniejszych przeglądarek internetowych a także za pomocą urządzeń mobilnych. Strona portalu musi być responsywna, dostosowując się do rozdzielczości urządzenia na jakim będzie oglądana. Portal musi zapewniać wielojęzyczność i być dostępny nie tylko w polskiej ale w innych wersjach językowych. Wymagana jest oprócz wersji polskiej minimum wersja anglojęzyczna. Każda publikowana informacja na łamach Portalu (niezależnie czy jest to dokument czy poszczególny wpis z Bazy Danych) musi mieć możliwość uzupełnienia o dodatkowy Formularz.
LICENCJE	Wraz z systemami należy dostarczyć wszystkie niezbędne systemy operacyjne środowisk pracy, bazy danych wraz z licencjami, niezbędne licencje oprogramowania umożliwiające świadczenie usług drogą elektroniczną oraz jeżeli wymagane licencje dostępowe.

2. SYSTEM ELEKTRONICZNEGO ZARZĄDZANIA DOKUMENTAMI

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY FUNKCJONALNE
WYMAGANIA OGÓLNE	Zadanie dotyczy 5 Jednostek Organizacyjnych Zamawiającego: 1) Zespół Szkół w Proszowicach 2) Zespół Szkół w Piotrkowicach Małych 3) Powiatowe Centrum Pomocy Rodzinie w Proszowicach 4) Zarząd Dróg Powiatowych w Proszowicach 5) Powiatowy Inspektorat Nadzoru Budowlanego w Proszowicach Zadanie obejmuje stworzenie instalacji wielojednostkowej systemu zarządzania dokumentami, która ma na celu udostępnienie jednostkom podległym (jednostki organizacyjne), systemu zarządzania dokumentami w pełnej funkcjonalności (w tym komunikacji z platformą ePUAP) wraz z możliwością wymiany dokumentów między jednostkami i urzędem bez konieczności budowania infrastruktury sprzętowej oraz ponoszenia dodatkowych kosztów związanych z administrowaniem i zabezpieczeniem danych w każdej z tych jednostek. Rozwiązanie musi umożliwiać w pełni elektroniczne procedowanie spraw pomiędzy Urzędem a Jednostkami Organizacyjnymi odpowiedzialną za realizację. Integracja uruchomionych systemów EZD z systemem EZD Zamawiającego musi być zrealizowana w sposób umożliwiający wymianę informacji i prowadzenie procesów elektronicznych pomiędzy nimi. Rozwiązanie musi umożliwiać Interesantom urzędu bieżące śledzenie stanu realizacji sprawy. Rozwiązanie musi być wykonany w architekturze trójwarstwowej. Rozwiązanie musi zapewniać przechowywanie plików dokumentów w bazie danych. Rozwiązanie musi wykorzystywać wspólne repozytorium dokumentów dla systemu zarządzania dokumentami i systemów dziedzinowych. Rozwiązanie musi zapewniać integrację z platformą ePUAP oraz z użytkowanym przez Zamawiającego systemem BIP w zakresie automatycznej publikacji rejestrów prowadzonych w systemie EZD. Rozwiązanie musi zapewniać integrację ze elektronicznymi skrzynkami podawczymi systemu ePUAP.
ZARZĄDZANIE DOKUMENTAMI	Obsługa spraw zgodnie z instrukcją kancelaryjną. Zakładanie i znakowanie spraw w oparciu o klasyfikację RWA. Obsługa elektronicznych teczek aktowych i spisów spraw. Dekretacja spraw na wydziały i osoby. Możliwość przypisywania uwag do spraw. Obsługa metryczki sprawy. Możliwość związania korespondencji /sprawy z obiektami w systemie dziedzinowym. Dostęp do udostępnianej dla danego systemu dziedzinowego listy spraw w ramach posiadanych uprawnień użytkownika. Wyszukiwarka spraw. Rejestrowanie korespondencji przychodzącej i wychodzącej z automatyczną numeracją. Wyszukiwarka korespondencji. Podgląd plików korespondencji przychodzącej.

	Dekretacja korespondencji na jednego lub wielu pracowników z jednoznacznym określeniem osoby odpowiedzialnej. Możliwość dekretacji na grupy pracowników. Możliwość automatycznej dekretacji na podstawie rodzaj korespondencji. Możliwość przypisywania uwag do korespondencji w trakcie dekretacji i niezależnie od niej. Możliwość zadekretowania wstępnego terminu załatwienia dla korespondencji. Historia dekretacji. Obsługa wielu miejsc rejestracji korespondencji. Obsługa wielu rejestrów korespondencji. Obsługa listy podmiotów powiązanych (osób fizycznych i/lub prawnych) z korespondencją. Możliwość rejestracji korespondencji e-mail bezpośrednio z programu. Możliwość rejestracji wysyłki korespondencji w jednej kopercie. Możliwość tworzenia specjalnie oznaczonych kopii korespondencji. Rejestracja korespondencji wychodzącej w oparciu o kody kreskowe. Obsługa definiowalnych, dodatkowych atrybutów korespondencji. Obsługa operacji zatwierdzania dokumentu własnego przez jednego lub wielu pracowników. Obsługa operacji potwierdzenia zapoznania się z dokumentem własnym przez pracownika. Automatyczne wersjonowanie przy edycji pliku zatwierdzonego. Dekretacja dokumentu własnego na jednego lub wielu pracowników z jednoznacznym określeniem osoby odpowiedzialnej. Możliwość przypisywania uwag do dokumentu własnego w trakcie dekretacji i niezależnie od niej Obsługa statusów dokumentów. Obsługa wielu rejestrów dokumentów. Automatyczne generowanie dokumentów na podstawie szablonów, Prosta edycja istniejących szablonów z poziomu programu. Obsługa definiowalnych, dodatkowych atrybutów dokumentów własnych. Obsługa listy podmiotów (osób fizycznych i/lub prawnych) powiązanych z danym dokumentem. Możliwość tworzenia specjalnie oznaczonych kopii dokumentów. Możliwość przekazywania dokumentów własnych do wysyłki do pracownika rejestrującego korespondencję wychodzącą. Zaawansowany system uprawnień - do folderów dokumentów, dokumentów, rodzajów spraw, funkcjonalności (role). Obsługa zastępstw. Logowanie kontekstowe do systemu. Możliwość prezentacji graficznej raportów w postaci wykresów. Wydruk kopert na podstawie informacji z dokumentów przeznaczonych do wysyłki.
INTEGRACJA	Pełna, dwukierunkowa integracja z ePUAP - aplikacja musi mieć możliwość integracji z platformą typu ESP, w tym co najmniej z ePUAP. Przedmiotem zamówienia jest uruchomienie integracji aplikacji z platformą ePUAP oraz weryfikacja Profilu Zaufanego ePUAP na żądanie użytkownika aplikacji. Zakres integracji to co najmniej:

	a. Pobieranie w sposób automatyczny przesyłek przychodzących do dowolnego konta/skrytki Zamawiającego na platformie ePUAP i zaciąganie ich do aplikacji. b. Wysyłanie z aplikacji w sposób automatyczny przesyłek wychodzących do dowolnych kont/skrytek interesantów Zamawiającego na platformie ePUAP, zarówno w trybie przedłożenia jak i doręczenia. W zakresie integracji z ePUAP, program musi umożliwiać co najmniej: a. zdefiniowanie maksymalnego odstępu czasu między kolejnymi automatycznymi wywołaniami pobierania przesyłek przychodzących oraz wysyłania przesyłek wychodzących z i do platformy ePUAP. Pobranie przesyłek przychodzących do aplikacji musi skutkować usunięciem tych przesyłek na platformie ePUAP z puli dostępnych do pobrania. b. udostępniać uprawnionym pracownikom listę przesyłek przychodzących, które wpłynęły z platformy ePUAP. Poszczególne przesyłki na tej liście muszą być opisane co najmniej następującymi parametrami: ▪ danymi konta/skrytki nadawcy w platformie ePUAP; ▪ rodzajem przesyłki (wskazanie wzoru dokumentu w CRWDE); ▪ datą i czasem wpływu przesyłki do konta/skrytki ePUAP, na podstawie momentu generacji UPO; ▪ unikalnym identyfikatorem przesyłki w aplikacji; ▪ plikami oryginału przesyłki przychodzącej oraz skojarzonym z nią plikiem UPO. c. na żądanie użytkownika generować i wyświetlać wizualizacje plików przesyłki przychodzącej lub wychodzącej oraz UPO, a także umożliwiać lokalny zapis lub wyświetlenie w skojarzonej z typem pliku aplikacji na klienckiej stacji roboczej. Użytkownik musi mieć możliwość lokalnego zapisu wizualizacji w formacie PDF. d. na żądanie użytkownika weryfikować podpis elektroniczny pod plikiem przesyłki elektronicznej oraz UPO. e. na żądanie użytkownika wyświetlać i udostępniać listę plików dołączonych do treści pliku przesyłki przychodzącej lub wychodzącej oraz umożliwiać lokalny zapis lub wyświetlenie w skojarzonej z typem pliku aplikacji na klienckiej stacji roboczej. f. umożliwiać w odniesieniu do każdej przesyłki przychodzącej z platformy ePUAP na liście co najmniej: ▪ rejestrację przesyłki przez uprawnionego użytkownika w Rejestrze Przesyłek Przychodzących – rejestracja przesyłki musi wiązać się ze wskazaniem: procesu w którym dana przesyłka zostanie obsłużona, wypełnieniem formularza rejestracji, odpowiedniej komórki lub stanowiska merytorycznego będącego odbiorcą przesyłki. ▪ rezygnację z rejestracji przesyłki – rezygnacja z rejestracji przesyłki musi wiązać się z nadaniem jej odpowiedniego statusu/oznaczenia, musi również istnieć możliwość powrotu do rejestracji przesyłki, wobec której uprzednio zrezygnowano z rejestracji. g. automatycznie rejestrować UPO jakie wpływają z platformy ePUAP do aplikacji. h. automatycznie i trwale kojarzyć ze sobą przesyłki przychodzące z platformy ePUAP albo wychodzące do platformy z dotyczącymi je UPO oraz udostępniać je razem na wszystkich listach aplikacji w sposób umożliwiający użytkownikowi łatwy dostęp do zarówno do przesyłki jak i UPO, w tym: ▪ przekazanie przesyłki przychodzącej komórce lub stanowisku merytorycznemu musi być jednoznaczne z przekazaniem dotyczącego jej UPO.

	▪ poświadczenia odbioru przesyłki wychodzącej (UPD, UPP) przyporządkowane do przesyłki wychodzącej muszą być dostępne z poziomu widoku szczegółów akt sprawy w sposób jasno przedstawiający przyporządkowanie do danej przesyłki wychodzącej/dokumentu. Poszczególne poświadczenia odbioru muszą być opisane co najmniej następującymi parametrami: - datą odbioru przesyłki wychodzącej; - datą wpływu poświadczenia do aplikacji; - danymi interesanta – adresata przesyłki wychodzącej; - numerem przesyłki wychodzącej w rejestrze przesyłek wychodzących. i. umożliwiać powiązanie przesyłki przychodzącej z platformy ePUAP z odpowiednim interesantem, utworzonym uprzednio albo tworzonego w momencie rejestracji przesyłki, na podstawie danych konta/skrytki nadawcy lub treści dokumentu lub danych podpisującego. j. wymagać od użytkowników rejestrujących przesyłki przychodzące wprowadzania informacji o konieczności odpowiedzi nadawcy w formie elektronicznej. k. umożliwiać pracownikom merytorycznym wysyłanie przesyłek wychodzących do kont/skrytek interesantów na platformie ePUAP. l. weryfikować rozmiar dokumentu przesyłanego z dopuszczalnymi limitami platformy ePUAP, przed wysłaniem przesyłki wychodzącej do platformy ePUAP oraz zgodność przesyłki ze wzorem dokumentu w CRWDE wraz z podpisem elektronicznym. Integracja z Portalem Interesanta w zakresie automatycznego (tj. bez udziału użytkowników) publikowania statusów prowadzonych spraw w Systemie Elektronicznego Zarządzania Dokumentami. Integracja z Portalem Interesanta w zakresie automatycznego (tj. bez udziału użytkowników) publikowania prowadzonych rejestrów w Systemie Elektronicznego Zarządzania Dokumentami.

3. SZKOLENIE W ZAKRESIE E-USŁUG

NAZWA KOMPONENTU	WYMAGANIA MINIMALNE
SZKOLENIA UŻYTKOWNIKÓW	Do każdego modułu wspomagającego obsługę obszarów działalności urzędu. Zamawiający wskaże osoby, które Wykonawca przeszkoli. Wykonawca zapewni dla każdego modułu odpowiednią ilość szkoleń, nie mniejszą jak 16 godzin, gwarantującą pracownikom na danym stanowisku sprawną obsługę rozwiązania. Potwierdzeniem odbycia szkolenia będzie protokół podpisany przez każdego pracownika. Szkolenia będą realizowane w pomieszczeniach i na sprzęcie udostępnionym przez Zamawiającego. Szkolenia muszą odbywać się w godzinach pracy Zamawiającego. Zamawiający dopuszcza możliwość przeprowadzania szkoleń „on-line" w zastępstwie szkoleń tradycyjnych. Dopuszcza się po uzgodnieniu z Zamawiającym przeprowadzenie szkoleń grupowych w wybranych obszarach tematycznych.

SZKOLENIA ADMINISTRATORÓW	Wykonawca przeszkoli osoby pełniące obowiązki administratorów wskazanych przez Zamawiający w zakresie zarządzania użytkownikami i uprawnieniami. zabezpieczania i odtwarzania danych. Wykonawca zapewni przeszkolenie administratora wskazanego przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanego systemu bazodanowego. Szkolenie musi obejmować co najmniej instalację. konfigurację bazy danych, obsługę narzędzi administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii.
DOKUMENTACJA POWYKONAWCZA SYSTEMU E-USŁUG	Wykonawca przed rozpoczęciem szkolenia dostarczy do każdego modułu będącego przedmiotem niniejszego zamówienia, dokumentację w języku polskim w postaci elektronicznej i papierowej (w ilości 1 sztuki), zawierającą : - opis ogólnych informacji o systemie (poruszanie się po systemie); - opis słowników aplikacji; - opis parametryzacji aplikacji możliwej do wykonania przez użytkowników merytorycznych – liderów, administratora; - opis wszystkich funkcji dostępnych w aplikacji; - opis wraz z procedurami instalacji i konfiguracji całego systemu – od instalacji systemu operacyjnego do uruchomienia aplikacji klienckiej na stanowisku użytkownika; - opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych; - plan odtwarzania systemu po awarii.

CZĘŚĆ II – ROZWIĄZANIA BEZPIECZEŃSTWA

WYMAGANIA GWARANCYJNE

Zamawiający wymaga minimum 60 miesięcy gwarancji na przedmiot zamówienia. Gwarancja musi uwzględniać automatyczne aktualizacje systemu oraz całodobowe wsparcie techniczne świadczone w języku polskim.

Okres gwarancji liczony będzie od daty sporządzenia protokołu odbiorczego przedmiotu zamówienia.

Produkty objęte przedmiotem zamówienia musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy. Zamawiający nie dopuszcza rozwiązań pochodzących z rynku wtórnego.

Rozwiązania muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

1. SYSTEM BADANIA PODATNOŚCI

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY FUNKCJONALNE
WYMAGANIA PODSTAWOWE	Istniejące rozwiązanie UTM Stormshield SN510 należy wyposażyć w system badania podatności. System badania podatności musi umożliwiać weryfikacje ruchu w sieci LAN pod kątem generujących go aplikacji, zwiększając ogólne bezpieczeństwo i ochronę danych zgodnie z wytycznymi KRI w zakresie ochrony przed nieuprawnionym ujawnianiem oraz RODO w zakresie ochrony treści.
FUNKCJONALNOŚĆ	Moduł musi wykrywać typu i wersję oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Musi wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu. Musi weryfikować czy wykryta aplikacja jest wrażliwa na ataki lub posiada inne luki bezpieczeństwa. Musi umożliwiać prezentację szczegółowej listy aplikacji sieciowych, pracujących na stacjach roboczych, jak np. przeglądarki internetowe, aplikacje do multimediów (streamingu audio/video), programy antywirusowe, itp. Kliknięcie na wskazaną przez narzędzie aplikację musi powodować wyświetlenie wszystkich komputerów, na których dany program został wykryty, a także pozwala sprawdzić wersję tej aplikacji. Musi wyszukiwać nieaktualne wersje oprogramowania na stacjach roboczych i serwerach. System musi umożliwiać automatyczne wysyłanie powiadomień o zagrożeniach wskazując zagrożone stacje robocze. System musi podawać źródła z których można pobrać odpowiednie poprawki i aktualizacje, które przywrócą optymalny poziom bezpieczeństwa.

2. SYSTEM DLP

Nazwa komponentu	Wymagane minimalne parametry funkcjonalne
INFORMACJE OGÓLNE	Musi zapewniać wsparcie instalacji w oparciu o relacyjną bazę danych. Praca w architekturze serwer, agent, klienta gdzie komunikacja serwera zarządzającego z klientem odbywa się tylko przy pomocy agenta. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych. Musi być w języku polskim. Możliwość aktualizacji komponentów własnych. Możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych oraz aplikacji. Musi być możliwość wyłączenia automatycznego pobierania. Możliwość dla konkretnej stacji wymuszenia komunikacji w czasie rzeczywistym w celu sprawdzania konfiguracji. Możliwość zablokowania/uruchomienia trybu awaryjnego na stacji końcowej Możliwość zdefiniowania portów dla ruchu pocztowego które mają być monitorowane przez oprogramowania zainstalowane na stacji końcowej. Możliwość ustawień powiadomień dla użytkownika końcowego w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. Możliwość audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, dokumenty drukowane, ruch sieciowy, wysyłane oraz odbierane wiadomości e-mail oraz wykonywane czynności na plikach. Możliwość filtrowania poprzez podanie zakresu czasu. Możliwość wykonania zadania tagowania plików, które już znajdują się na stacjach roboczych i zasobach sieciowych ale również nowych plików, które powstaną na bazie istniejących plików z tagami. Możliwość analizy lub tagowania nowo powstałych plików wrażliwych w oparciu o: – Aplikację z której zostały utworzone – Lokalizację lokalną oraz sieciową – Adres URL, z którego został pobrany plik – Format pliku – Zawartość pliku Możliwość analizy lub tagowania posiadanych plików wrażliwych w oparciu o: – Lokalizację lokalną oraz sieciową – Format pliku – Zawartość pliku Możliwość tagowania plików w oparciu o ich zawartość, m.in. o: – Numery Kart kredytowych – Numer PESEL – Numer polskiego dowodu osobistego – Wyrażenia regularne – Określone ciągi znaków – Numer IBAN Możliwość powiadamiania użytkownika jeśli zidentyfikuje w wiadomości e-mail m.in.: – Numery Kart kredytowych

	– Numer PESEL – Numer polskiego dowodu osobistego – Wyrażenia regularne – Określone ciągi znaków – Numer IBAN Możliwość powiadamiania użytkownika jeśli zidentyfikuje w załączniku do wiadomości e-mail m.in.: – Numery Kart kredytowych – Numer PESEL – Numer polskiego dowodu osobistego – Wyrażenia regularne – Określone ciągi znaków – Numer IBAN Dla tagowanych plików możliwość utworzenia reguł w oparciu o czynności: a) Blokowania oraz zezwalania na zapisywanie, przenoszenie plików do lokalizacji na dyskach lokalnych lub konfiguracji określonych lokalizacji, do której będzie możliwość bądź nie będzie możliwości zapisu. b) Blokowania oraz zezwalania na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń. c) Możliwości zabezpieczenia możliwości drukowania, utworzenia białej oraz czarnej listy drukarek. d) Blokowania oraz zezwalania na zapisywanie, przenoszenie do lokalizacji sieciowej oraz określenie białej oraz czarnej listy lokalizacji sieciowych. e) Blokowania oraz zezwalania wysyłki plików za pośrednictwem klientów pocztowych oraz określenia białej oraz czarnej listy adresów e-mail oraz domen. f) Blokowania oraz zezwalania na zapisywanie, przenoszenie plików na dyski zaszyfrowane w oparciu o lokalnie zaszyfrowane dyski oraz zewnętrzne zaszyfrowane dyski. g) Blokowania oraz zezwalania na zapisywanie, przenoszenie plików do folderów synchronizacji z usługami chmury (Google Drive, OneDrive Business, One Drive Personal, Dropbox, Box Sync, SharePoint). h) Blokowania oraz zezwalania na zapisywanie, przenoszenie plików poprzez usługę pulpitu zdalnego i) Blokowania oraz zezwalania na wykonywanie zrzutów ekranowych, skopiowania zawartości, nagrywania na płyty CD/DVD oraz wirtualnego drukowania plików. j) Uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje. Możliwość określenia stref urządzeń pamięci masowej, Możliwość globalnego zablokowania oraz zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury (Google Drive, OneDrive Business, One Drive Personal, Dropbox, Box Sync, SharePoint). Możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzowanie do zaszyfrowanych nośników wymiennych musi być w pełni niezauważalne dla użytkownika. Możliwość tworzenia kluczy szyfrujących które będą kompatybilne z funkcjonalnością BitLocker dla zapewnienia transparentności współdzielenia zaszyfrowanych nośników wymiennych. Możliwość globalnego zablokowania, zezwolenia, dostępu tylko do odczytu z korzystania z określonych urządzeń podłączanych do portu USB, urządzeń

	przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT. Możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM. Możliwość wygenerowania hasła ratunkowego do odblokowania dostępu do zaszyfrowanych dysków oraz dysków wymiennych, w sytuacji jeżeli użytkownik zapomni hasła. Możliwość blokowania stron internetowych w oparciu o kategorię stron oraz po podaniu adresu URL. Musi istnieć możliwość konfiguracji przekierowania z dowolnej strony która została zablokowana. Możliwość blokowania aplikacji w oparciu o kategorię aplikacji, lokalizację aplikacji oraz aplikację ze sklepu Windows. Możliwość blokowania możliwości drukowania na wszystkich oraz określonych drukarkach fizycznych, sieciowych oraz wirtualnych. Musi także posiadać możliwość ograniczenia drukowania per limit stron na dzień, tydzień oraz miesiąc.
RAPORTOWANIE	Możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, dokumenty drukowane, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach. Możliwość raportowania reguł bezpieczeństwa w oparciu o incydenty na plikach chronionych, ogółu wykonanych operacji na plikach, podsumowania wszystkich incydentów bezpieczeństwa, akcji użytkowników na zabezpieczonych plikach, zablokowanych operacji na dyskach lokalnych, zewnętrznych, podsumowanie korzystania z urządzeń oraz ich typów. Możliwość utworzenia raportu w oparciu o użycie aplikacji, zablokowanych aplikacji, zablokowanych drukarek, podsumowanie drukowania, zablokowane strony internetowe, zablokowanych użytkowników, aktywność użytkowników na serwerze, alarmy, ustawień klienta, kopii bezpieczeństwa, zarządzania stacjami końcowymi, dezaktywacją licencji oraz zaawansowanego debugowania. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu. Raporty muszą być generowane do pliku PDF, XLS po podaniu lokalizacji zapisywanego pliku, na wskazane adresy e-mail.
ADMINISTRACJA	Synchronizacja użytkowników oraz stacji roboczych z usługą Active Directory. Możliwość zarządzania bazą danych poprzez określone zadania – kopii bazy danych, kopii oraz usunięcia bazy danych, usunięcia bazy danych, ustawieniach kopii bazy danych - dostępne z poziomu konsoli wraz z określeniem automatycznego powtarzania zadań: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące. Możliwość zdefiniowania w programie przedziału czasowego dla kopii zapasowej bazy programu. Funkcje automatycznej kopii bazy danych programu DLP co 7, 14, 30 dni Możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania. Możliwość zmiany hasła oraz loginu innego administratora. Możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Możliwość logowania za pośrednictwem grup domenowych administratorów.

	możliwość ustawienia godzin w których nie będą obowiązywały użytkowników reguły kontroli aplikacji oraz stron internetowych. Godziny pracy muszą być ustalane dla poszczególnych dni tygodnia. Możliwość określenia czy dokumenty zawierające dane wrażliwe takie jak numery Kart kredytowych, numer PESEL, numer polskiego dowodu osobistego, wyrażenia regularne, określone ciągi znaków, numer IBAN, mogą zostać przesłane do chmur lub innych źródeł WWW. Możliwość określenia bezpiecznych stref oraz domen do których pliki mogą zostać przesłane. Możliwość określenia czy dokumenty mogą zostać przesłane przez komunikatory niezależnie od zawartości plików. Lista komunikatorów musi wspierać przynajmniej Skype, GG, ICQ,Facebook Messenger. Możliwość określenia czy dokumenty zawierające dane wrażliwe takie jak numery Kart kredytowych, numer PESEL, numer polskiego dowodu osobistego, wyrażenia regularne, określone ciągi znaków, numer IBAN, mogą zostać przesłane przez komunikatory. Lista komunikatorów musi wspierać przynajmniej Skype, GG, ICQ,Facebook Messenger. Możliwość określenia czy dokumenty zawierające dane wrażliwe takie jak numery Kart kredytowych, numer PESEL, numer polskiego dowodu osobistego, wyrażenia regularne, określone ciągi znaków, numer IBAN, mogą zostać przesłane na urządzenia zewnętrzne. Możliwość przygotowania pliku instalacyjnego agenta. Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu. Możliwość wysyłania alarmów w oparciu o odmowę dostępu dla użytkownika do lokalizacji sieciowych, stron internetowych, aplikacji, do pliku, folderu, zablokowana możliwość przenoszenia oraz kopiowania danych, podłączone nieznane urządzenie, połączone urządzenie zostało zablokowane, nowa drukarka została połączona, została przekroczona liczba stron drukowania, drukowanie zostało zablokowane. Pliki posiadające tag były kopiowane na dysk USB, wysyłane za pośrednictwem wiadomości e-mail.
KONSOLA ZDALNA	Możliwość przeglądania informacji dotyczących bezpieczeństwa w oparciu o próby wycieku danych, operacji na plikach posiadających tag, plików wysyłanych do sieci, plików pobieranych z sieci, plików wysyłanych drogą e-mailową, plików kopiowanych na dyski zewnętrzne, pliki drukowane. Konsola webowa musi umożliwiać obserwację produktywności pracy użytkowników w oparciu o zdefiniowane przez administratora aplikacje oraz strony internetowe. Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu. Możliwość instalacji na systemach Windows Server 2008 R2 lub nowszych. Możliwość współdziałania z bazą danych MS SQL Server 2012 i nowszymi. Logowanie do konsoli webowej musi opierać się na wcześniej utworzonych kontach użytkowników w konsoli aplikacyjnej. Uprawnienia dostępu wybranych użytkowników do poszczególnych informacji na temat grup komputerów lub grupy użytkowników w konsoli webowej, muszą być ustalane z poziomu konsoli aplikacyjnej. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:

	a) Bezpieczeństwo danych: • Przegląd informacji o incydentach bezpieczeństwa. • Przegląd danych przychodzących. • Przegląd danych wychodzących. • Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików. • Podłączane/odłączane urządzenia przenośne. b) Produktywność: • Przegląd informacji na temat produktywności użytkowników. • Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji. • Trendy c) Eksploatacja sprzętu: • Przegląd informacji na temat eksploatacji sprzętu komputerowego. • Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery. • Eksploatacja drukarek. • Eksploatacji sieci. Możliwość dodania klucza licencji. Możliwość konfiguracji/zmiany domyślnego serwera SMTP. Możliwość weryfikacji wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania. Możliwość generowania raportów z danymi na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu. Raporty muszą być generowane dla wybranych grup komputerów/użytkowników w interwałach tygodniowych lub miesięcznych. Raporty będą przesyłane drogą e-mailową.
INNE	Zamawiający wymaga instalacji rozwiązania na serwerze udostępnionym wykonawcy, konfiguracji i uruchomienia. Instalacja musi obejmować również minimum 10 stacji komputerowych. W ramach konfiguracji Zamawiający wymaga: – włączenie funkcji audytora, – ustawienie tagowania minimum jednej przykładowej ścieżki lokalnej w oparciu o minimum 10 plików tekstowych, – ustawienie kategorii danych w oparciu o wskazane przez klienta dane wrażliwe, – ustawienie reguł DLP, Wykonawca przeprowadzi instruktarz dla administratora Zamawiającego w zakresie w/w zagadnień, w stopniu umożliwiającym administratorowi samodzielną konfigurację i administrację rozwiązania. Instruktarz musi obejmować omówienie funkcji konsoli rozwiązania.