RGK.ZP.271.15.2022

Część II SWZ – Opis Przedmiotu Zamówienia

Dla Części I Zamówienia

Wymagana specyfikacja techniczna

1. Serwer główny dla Urzędu Gminy Mysłakowice – 1 sztuka	Nazwa producenta / Model_____/_____

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Tower z możliwością instalacji min 8 dysków twardych 3,5”.
Płyta główna	Z możliwością instalacji dwóch fizycznych procesorów, posiadająca minimum 16 slotów na pamięć RAM RDIMM z możliwością zainstalowania do minimum 1TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Zainstalowany jeden procesor min. 8-rdzeniowe, min. 2.1GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 83.8 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
Pamięć RAM	32 GB pamięci RAM UDIMM o częstotliwości taktowania minimum 3200MHz
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum 5 slotów PCI Express trzeciej generacji
Wbudowane porty	Minimum 8 portów USB z czego min. 3 w technologii 3.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 1x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum dwa interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCI Express oraz złącz USB.
Kontroler pamięci masowej	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Wewnętrzna pamięć masowa	Możliwość instalacji dysków twardych 3,5” typu: SATA, NearLine SAS, SAS, SSD. Zainstalowane 6 dysków SSD SATA o pojemności min. 960GB 10K Hot-Plug Możliwość instalacji dodatkowej wewnętrznej pamięci masowej typu flash, dedykowanej dla hypervisora wirtualizacyjnego, wyposażonej w 2 nośniki typu flash o pojemności min. 32GB, umożliwiającej konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości minimalnej ilości wewnętrznej pamięci masowej w serwerze. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 240GB oraz możliwość konfiguracji w RAID1.
System operacyjny/dodatkowe oprogramowanie	Windows Server 2022 Standard Dodatkowo należy dostarczyć: 45x licencja Windows Server 2022/2019 User CALs 10x licencja Windows Server 2022 RDS, User
Diagnostyka i bezpieczeństwo	- możliwość wyposażenia w moduł TPM 2.0 - wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Chłodzenie i zasilanie	Wentylator, zasilacze o mocy minimum 495W (redundantne) wraz z kablami zasilającymi.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ▪ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ▪ wsparcie dla IPv6; ▪ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ▪ integracja z Active Directory; ▪ wsparcie dla dynamic DNS; ▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ▪ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ▪ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Gwarancja	3-letnia gwarancja producenta realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie najnowszych uaktualnień oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (dokumenty załączyć do oferty) Serwer musi posiadać deklaracja CE (dokument załączyć do oferty) Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019.

2. Serwer zapasowy dla Urzędu Gminy Mysłakowice – 1 sztuka	Nazwa producenta / Model_____/_____

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Tower z możliwością instalacji min 8 dysków twardych 3,5”.
Płyta główna	Z możliwością instalacji dwóch fizycznych procesorów, posiadająca minimum 16 slotów na pamięć RAM RDIMM z możliwością zainstalowania do minimum 1TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Zainstalowany jeden procesor min. 8-rdzeniowe, min. 2.1GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 83.8 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
Pamięć RAM	32 GB pamięci RAM UDIMM o częstotliwości taktowania minimum 3200MHz
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum 5 slotów PCI Express trzeciej generacji
Wbudowane porty	Minimum 8 portów USB z czego min. 3 w technologii 3.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 1x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum dwa interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCI Express oraz złącz USB.
Kontroler pamięci masowej	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Wewnętrzna pamięć masowa	Możliwość instalacji dysków twardych 3,5” typu: SATA, NearLine SAS, SAS, SSD. Zainstalowane 2 dyski SSD SATA o pojemności min. 960GB 10K Hot-Plug Możliwość instalacji dodatkowej wewnętrznej pamięci masowej typu flash, dedykowanej dla hypervisora wirtualizacyjnego, wyposażonej w 2 nośniki typu flash o pojemności min. 32GB, umożliwiającej konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości minimalnej ilości wewnętrznej pamięci masowej w serwerze. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 240GB oraz możliwość konfiguracji w RAID1.
System operacyjny/dodatkowe oprogramowanie	Windows Server 2022 Standard Dodatkowo należy dostarczyć: 20x licencja Windows Server 2022/2019 User CALs 3x licencja Windows Server 2022 RDS, User
Diagnostyka i bezpieczeństwo	- możliwość wyposażenia w moduł TPM 2.0 - wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Chłodzenie i zasilanie	Wentylator, zasilacze o mocy minimum 495W (redundantne) wraz z kablami zasilającymi.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ▪ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ▪ wsparcie dla IPv6; ▪ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ▪ integracja z Active Directory; ▪ wsparcie dla dynamic DNS; ▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ▪ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ▪ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Gwarancja	Minimum 2-letnia gwarancja producenta realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie najnowszych uaktualnień oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (dokumenty załączyć do oferty) Serwer musi posiadać deklaracja CE (dokument załączyć do oferty) Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019.

3. Serwer baz danych dla Gminnego Ośrodka Pomocy Społecznej w Mysłakowicach – 1 sztuka	Nazwa producenta / Model_____/_____

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Tower z możliwością instalacji min 8 dysków twardych 3,5”.
Płyta główna	Z możliwością instalacji dwóch fizycznych procesorów, posiadająca minimum 16 slotów na pamięć RAM RDIMM z możliwością zainstalowania do minimum 1TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Zainstalowany jeden procesor min. 8-rdzeniowe, min. 2.1GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 83.8 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
Pamięć RAM	32 GB pamięci RAM UDIMM o częstotliwości taktowania minimum 3200MHz
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum 5 slotów PCI Express trzeciej generacji
Wbudowane porty	Minimum 8 portów USB z czego min. 3 w technologii 3.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 1x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum dwa interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCI Express oraz złącz USB.
Kontroler pamięci masowej	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Wewnętrzna pamięć masowa	Możliwość instalacji dysków twardych 3,5” typu: SATA, NearLine SAS, SAS, SSD. Zainstalowane 2 dyski SSD SATA o pojemności min. 960GB 10K Hot-Plug Możliwość instalacji dodatkowej wewnętrznej pamięci masowej typu flash, dedykowanej dla hypervisora wirtualizacyjnego, wyposażonej w 2 nośniki typu flash o pojemności min. 32GB, umożliwiającej konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości minimalnej ilości wewnętrznej pamięci masowej w serwerze. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 240GB oraz możliwość konfiguracji w RAID1.
System operacyjny/dodatkowe oprogramowanie	Windows Server 2022 Standard Dodatkowo należy dostarczyć: 20x licencja Windows Server 2022/2019 User CALs 3x licencja Windows Server 2022 RDS, User
Diagnostyka i bezpieczeństwo	- możliwość wyposażenia w moduł TPM 2.0 - wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Chłodzenie i zasilanie	Wentylator, zasilacze o mocy minimum 495W (redundantne) wraz z kablami zasilającymi.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ▪ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ▪ wsparcie dla IPv6; ▪ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ▪ integracja z Active Directory; ▪ wsparcie dla dynamic DNS; ▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ▪ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ▪ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Gwarancja	Minimum 2-letnia gwarancja producenta realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie najnowszych uaktualnień oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (dokumenty załączyć do oferty) Serwer musi posiadać deklaracja CE (dokument załączyć do oferty) Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019.

4. Stacje robocze (komputery) dla Urzędu Gminy Mysłakowice - 15 sztuk	Nazwa producenta / Model_____/_____

Komponent	Minimalne wymagania
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych. Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 8800 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php na dzień 01.02.2022
Pamięć RAM	16GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB. Jeden slot DIMM wolny.
Pamięć masowa	Dysk M.2 SSD 512GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”
Wydajność grafiki	Zintegrowana karta graficzna osiągająca w teście Passmark G3D Mark, w kategorii Average G3D Mark wynik co najmniej 1250 pkt. według wyników opublikowanych na stronie https://www.videocardbenchmark.net/gpu_list.php w dniu 17.12.2021
Wyposażenie multimedialne	Karta dźwiękowa min. czterokanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out.
Obudowa	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 mm. Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku, kiedy u producenta występuje kilka zasilaczy które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy. Wydruki 80plus musza być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera, iż wskazane zasilacze przez wykonawcę spełniają 80plus. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.

Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
System operacyjny oraz pakiet biurowy	Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. Pakiet office 2021 lub nowszy w wersji dla biznesu (wersja z wieczystą licencją)
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) Deklaracja zgodności CE (załączyć do oferty) Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów

	środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram.
Wymagania dodatkowe	Wbudowane porty: • 1 x HDMI 1.4 • 1 x DisplayPort 1.4 • 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: o Panel przedni: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 o Panel tylny: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 • 1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu • 1 x port audio-out na tylnym panelu obudowy • 1 x RJ – 45 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), Karta WLAN 2x2 802.11ax z Bluetooth w wersji nie niższej niż 5.0 montowana w dedykowanym slocie M.2 na płycie głównej. Nie dopuszcza się kart zajmujących slot PCIe. Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz USB z sześcioma klawiszami oraz rolką (scroll) Nagrywarka DVD +/-RW o prędkości min. 8x Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 26 dB (załączyć oświadczenie producenta
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji	Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Minimalny czas trwania gwarancji producenta wynosi 2 lata, z możliwością odpłatnego przedłużenia tego okresu do 5 lat od daty dostawy. Sposób realizacji usług wsparcia technicznego: • Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. • Dedykowany bezpłatny portal online producenta do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. • Opcjonalna pomoc techniczna za pośrednictwem czat online. Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.

	W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Dodatkowe oprogramowanie	Wykonawca dostarczy wraz z komputerem oprogramowanie producenta komputera które umożliwia pełne zarządzanie, monitoring, konfigurację a w szczególności: dystrybucję ustawień BIOS (zawierającego wcześniej zdefiniowane ustawienia jednakowe dla wszystkich), jednocześnie na wszystkich komputerach zgodnie z polityką bezpieczeństwa Zamawiającego. Oprogramowanie musi w pełni integrować się z Microsoft SCCM Wykonawca dostarczy sterowniki w formacie dedykowanym dla Microsoft SCCM w celu dystrybucji za pomocą dołączonego oprogramowania producenta komputera zgodnie z polityką bezpieczeństwa Zamawiającego. Zamawiający oczekuje oprogramowania zarządzającego produkowanego przez producenta i instalowanego przez producenta na etapie produkcji komputera. Program ma umożliwiać przynajmniej: - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.
MONITOR	Przekątna ekranu min 24" Rozdzielczość 1920 x 1080 (FullHD) Format 16:9 Ekran Płaski Powłoka matrycy Matowa Typ matrycy TN Rodzaj podświetlenia LED Czas reakcji 1 ms Częstotliwość odświeżania min 75 Hz Jasność min 250 cd/m2 Kontrast statyczny 1000:1 Kąt widzenia (poziomy/pionowy) 170°/160° Rozmiar plamki 0.277 Liczba wyświetlanych kolorów 16.7 mln Technologia ochrony oczu Redukcja migotania, Redukcja niebieskiego światła Złącza Podstawowe złącza D-Sub (VGA) x1, DisplayPort x1, HDMI x1 Hub USB USB 2.0 Wbudowane urządzenia Wbudowane głośniki 2 W Obrotowy ekran (PIVOT) Tak Możliwość montażu na ścianie (VESA) Tak Regulacja wysokości Tak

	Normy i standardy Nowa klasa energetyczna E *Preferowany model B2483HSU-B5*

Część II SWZ – Opis Przedmiotu Zamówienia

Dla Części II Zamówienia

Przedmiotem zamówienia jest dostawa obejmująca zakresem rzeczowym rozbudowę w Urzędzie Gminy Mysłakowice otwartej platformy e-usług https://eurzad.myslakowice.pl integrującej referencyjne i dziedzinowe zasoby informacyjne o charakterze opisowym w celu ich publikacji oraz świadczenia związanych z nimi usług, modernizację programów dziedzinowych umożliwiających świadczenie e-usług; wdrożenie formularzy e-usług; wdrożenie elektronicznego zarządzania dokumentacji (EZD) poprzez rozbudowę eKancelarii; rozbudowa aplikacji mobilnej; oraz przeprowadzenie szkoleń administratorów i użytkowników zaawansowanych.

Zakres rzeczowy zamówienia:

1. Uruchomienie i skonfigurowanie systemu Elektronicznego Zarządzania Dokumentacją (EZD):
    - Zaimplementowanie struktury organizacyjnej
    - Wprowadzenie użytkowników wraz z uprawnieniami
    - Konfiguracja sprzętu (drukarka, skaner, czytnik)
    - Integracja z ePUAP
    - Integracja z eNadawcą (Poczta Polska)
    - Integracja z INFO+ umożliwiająca automatyzację wysyłania decyzji podatkowych
    - Uruchomienie przykładowych rejestrów
    - Integracja z pieczęcią kwalifikowaną
    - Wprowadzenie przykładowych szablonów dokumentów
    - Zaimplementowanie schematów obiegu faktur
    - System instalowany w zasobach Gminy (serwer) albo na zasobach Wykonawcy
2. Szkolenia z systemu
    - 6 dni szkolenia stacjonarnego dla systemu EZD
    - 2 2 dni szkolenia stacjonarnego dla dodatkowych funkcjonalności portalu e-Urząd
3. Wsparcie i aktualizacja
    - Wsparcie i aktualizacja systemu EZD
    - Wsparcie i aktualizacja pieczęci kwalifikowanej
4. Dokumentacja
    - Audyt obecnych procedur obowiązujących w urzędzie oraz opracowanie dokumentacji przygotowującej do wdrożenia systemu EZD w jednostce
    - Szkolenie – przygotowanie do wdrożenia/instrukcja kancelaryjna
5. Funkcjonalności portalu e-Urząd
    - Uruchomienie modułu Rezerwacji Wizyt
    - Uruchomienie modułu Konsultacje Społeczne
    - Uruchomienie aplikacji mobilnej minstytucja
    - Uruchomienie modułu Płatności Online
6. Wsparcie i aktualizacja funkcjonalności portalu e-Urząd
    - Wsparcie i aktualizacja modułu Rezerwacji Wizyt
    - Wsparcie i aktualizacja modułu Konsultacje Społeczne
    - Wsparcie i aktualizacja aplikacji mobilnej minstytucja
7. E-formularze
    - Zamówienie nowych e-Formularzy
    - Przygotowanie plików formularzy
    - Przygotowanie wzorów formularzy do publikacji w CRWDE
    - Umieszczenie formularzy w portalu urzędu lub/i ePUAP

Wymagana specyfikacja funkcjonalna systemu teleinformatycznego e-Urząd i Elektronicznego Zarządzania Dokumentacją

Administracja Systemem teleinformatycznym e-Urząd

I. Ustawienia Portalu e-Urząd

1. Portal e-Urząd powinien mieć dostępną opcję włączenia i wyłączenia map prezentujących nieruchomości na mapie geograficznej.
2. Portal e-Urząd powinien umożliwiać zarządzenie widocznością poszczególnych usługi i modułów w portalu i aplikacji mobilnej w menu głównym, takimi jak płatności, szczegóły podatków, w zakresie włączania i wyłączania (dostępności i niedostępności).
3. Portal e-Urząd powinien umożliwiać zarządzanie komunikatami systemowymi poprzez:
   3.1. edycję komunikatów wyświetlanych użytkownikowi końcowemu w przypadku np. braku komunikacji z SD lub braku dostępności usług sieciowych z serwerów centralnych (ePUAP, PZ),
   3.2. logowanie wystąpienia wyświetleń takich komunikatów,
   3.3. przeglądanie przez Administratora logów z możliwością ustalenia użytkownika, czasu oraz lokalizacji (url) gdzie dany komunikat został wyświetlony.
4. Portal e-Urząd powinien umożliwiać pełne zarządzanie linkami (odnośnikami) na stronie logowania i stronie głównej dostępnej po zalogowaniu, w zakresie:
   4.1. umieszczania dowolnych linków i umieszczania ich w dowolnej kolejności w stosunku do już istniejących tam linków,
   4.2. reorganizacji istniejących i nowych linków.
5. Portal e-Urząd powinien umożliwiać zmianę herbu Gminy oraz charakterystyki kolorystycznej całego interfejsu dostępnego dla użytkownika końcowego w portalu i aplikacji mobilnej.
6. Portal e-Urząd powinien umożliwiać edycję treści tekstów udostępnianych na portalu, w szczególności klauzuli informacyjnej oraz deklaracji dostępności.
7. Portal e-Urząd powinien umożliwiać Administratorowi Systemu e-Urząd nadawanie uprawnień pracownikom urzędu do zarządzania poszczególnymi modułami w panelu administratora.
8. Portal e-Urząd powinien umożliwiać wpisanie dane kontaktowe Urzędu, które będą się wyświetlać w formularzu kontaktowym portalu oraz w aplikacji mobilnej.

II. Aktualności

1. Portal e-Urząd powinien umożliwiać publikowanie aktualności oraz zarządzanie nimi.
2. Opublikowane aktualności powinny być dostępne również dla użytkowników niezalogowanych.

III. Powiadomienia

1. Portal e-Urząd powinien umożliwiać wysyłanie powiadomień zwykłych (newsletter) oraz powiadomień automatycznych.
2. Portal e-Urząd powinien umożliwiać wysyłanie powiadomień kanałami e-mail, SMS lub PUSH.
3. Portal e-Urząd powinien umożliwiać Administratorowi wybór jakim kanałem ma zostać wysłane powiadomienie.
4. Portal e-Urząd powinien umożliwiać zarządzanie powiadomieniami (**newsletter**) w zakresie wysyłanych treści oraz zarządzanie bazą subskrybentów.
5. Portal e-Urząd powinien umożliwiać wysłanie newsletterów do grup subskrybentów w zależności od wybranych przez nich tematyki – np. wydarzenia kulturalne w gminie.
6. Portal e-Urząd powinien umożliwiać ustawienie daty i godziny wysyłki powiadomień.
7. Portal e-Urząd powinien posiadać logi o wysłanych powiadomieniach.
8. Portal e-Urząd powinien umożliwiać konfigurację powiadomień o płatnościach zbliżających się i zaległych (**powiadomienia automatyczne)** w zakresie:
   8.1. włączenia i wyłączenia funkcjonalności dla użytkownika końcowego,
   8.2. ustawienia liczby dni wysłania wiadomości przed terminem płatności,
   8.3. ustawienia liczby dni wysłania wiadomości po terminem płatności,

IV. e-Usługi

1. Portal e-Urząd powinien umożliwiać wprowadzenie pełnej karty usług z poziomu Panelu Administracyjnego. Treść karty usługi powinna być dostępna z poziomu portalu i aplikacji mobilnej.
2. Portal e-Urząd powinien umożliwiać wskazanie jednej lub wielu skrytek dla pojedynczego formularza. W przypadku podania wielu skrytek musi być możliwość wybrania skrytki, z której UPP zostanie przekazanie zwrotnie do użytkownika końcowego.
3. Portal e-Urząd powinien umożliwiać ustawienie statusu „ukryty" i „aktywny". W przypadku statusu „ukryty" formularz będzie widoczny dla pracowników urzędu w pełnym zakresie bez konieczności publikowania go dla wszystkich użytkowników końcowych. W przypadku statusu „aktywny" formularz będzie dostępny dla wszystkich użytkowników.
4. Portal e-Urząd powinien umożliwiać ustawienie zakresu dostępności e-Usługi w portalu lub aplikacji mobilnej.
5. Portal e-Urząd musi umożliwić publikację listy formularzy również dla użytkowników niezalogowanych.
6. Portal e-Urząd powinien umożliwiać przypisanie do formularza dowolnego wzoru z CRWDE.
7. Portal e-Urząd powinien umożliwiać przypisywanie poszczególnych formularzy do kategorii tematycznych i ich przeglądanie przez użytkownika końcowego z podziałem na te kategorie.
8. Portal e-Urząd powinien dać wgląd do pism wysłanych przez Użytkownika, w szczególności powinny się wyświetlać; UPP, podgląd pisma, data wysłania, dane użytkownika wysyłającego pismo.

V. Obsługa Kont Firmowych

1. Portal e-Urząd powinien umożliwiać rozpatrywanie wniosków o dostęp do Konta Firmowego dla osób prawnych.
2. Portal e-Urząd powinien powiadamiać wskazanych w Systemie e-Urząd pracowników urzędu, którzy zostaną poinformowani o nowym wniosku o dostęp do Konta Firmowego.
3. Portal e-Urząd powinien udostępniać narzędzie, za pomocą którego pracownik urzędu w łatwy sposób ustali czy wnioskodawca oraz osoby, które mają mieć dostęp do Konta Firmowego, posiadają już konta w Systemie e-Urząd. Portal e-Urząd automatyczne powiadomi wnioskodawcę o rezultacie rozpatrzenia wniosku w wiadomości e-mail.

VI. Płatności

1. Portal e-Urząd powinien umożliwiać przegląd wszystkich dokonanym w portalu lub aplikacji mobilnej płatności z możliwością przefiltrowania wg: użytkownika, unikalnego identyfikatora płatności, kwocie, statusie płatności, kanału płatności.
2. Portal e-Urząd powinien wyświetlać szczegóły każdego koszyka.

VII. Użytkownicy

1. Portal e-Urząd musi posiadać listę wszystkich użytkowników, którzy zalogowali się do Systemu e-Urząd.
2. Lista użytkowników powinna wyświetlać informacje:
   2.1. Imię,
   2.2. Nazwisko,
   2.3. Adres e-mail,
   2.4. Login ePUAP,
   2.5. PESEL,
   2.6. Aktualny stan zgód na doręczenia pism drogą elektroniczną do urzędu,
   2.7. Kanał komunikacji (Portal/aplikacja mobilne/oba).
3. Portal e-Urząd musi posiadać narzędzie do nadawania uprawnień Administratora w całości lub w części dla danego użytkownika.
4. Portal e-Urząd musi mieć historię wysłanych zgód o doręczeniach elektronicznych dla każdego użytkownika, która uwzględnia wszystkie kanały wprowadzenia zgody do systemu – portal, aplikacja mobilna lub ręczne przez pracownika urzędu poprzez system EZD.
5. Portal e-Urząd musi mieć możliwość czasowego lub trwałego zablokowania Użytkownika.

6. Portal e-Urząd musi wyświetlać informacje o urządzeniach na jakich Użytkownicy zainstalowali aplikację mobilną.

IX. Monitorowanie

1. Portal e-Urząd powinien posiadać funkcjonalność umożliwiającą stałe monitorowanie najważniejszych usług w systemie i powiadamiającą mailowo administratora o błędach w systemie (np. zerwanie połączenia VPN, brak dostępności Profilu Zaufanego).
2. Portal e-Urząd powinien umożliwiać przeglądanie logów w zakresie dostępności:
   2.1. domeny www,
   2.2. SSO – w ramach PZ i KWT,
   2.3. PZ – w zakresie podpisywania dokumentów Podpisem Zaufanym,
   2.4. ESP – wszystkich zdefiniowanych w Systemie e-Urząd skrytek urzędu w ramach ESP ePUAP,
   2.5. VPN – wymaganego połączenia przy pobieraniu danych z SD,
   2.6. SD – dostępności API SD.
3. Portal e-Urząd powinien umożliwiać uruchomienie powiadomień dla Administratorów w sytuacji, kiedy którykolwiek z monitorowanych elementów zmieni status z „dostępny" na „niedostępny" oraz w odwrotnym kierunku.

X. Umawianie Wizyt

1. Portal e-Urząd powinien umożliwiać tworzenie oraz zarządzanie dowolną liczbą kalendarzy dla komórek organizacyjnych Urzędu, przy czym dla pojedynczej komórki można utworzyć co najmniej jeden kalendarz, przy czym utworzenie kalendarza wymaga:
   1.1. nazwy komórki organizacyjnej
   1.2. lokalizacji (adres)
   1.3. opisu zakresu działalności
   1.4. wskazania z listy użytkowników systemu e-Urząd użytkowników co najmniej jednego pracownika Urzędu który będzie miał uprawnienia do zarządzania kalendarzem i wizytami (Zarządzający).
2. Portal e-Urząd powinien umożliwiać konfigurację modułu umawiania wizyt, tym:
   2.1. Oznaczać dostępny kanał wysyłki powiadomień (e-mail lub SMS),
   2.2. Ustalać czy na wizytę może się umówić Użytkownik zalogowany lub niezalogowany,
   2.3. Ustawić limit wizyt Użytkownika na dzień,
   2.4. Ustawić ilość dni wyprzedzenia do umówionej wizyty,
   2.5. Zarządzać interwałami wizyt, przy czym każdy interwał wymaga obligatoryjnie wskazania;
      2.5.1. daty wizyty
      2.5.2. godziny rozpoczęcia
      2.5.3. godziny zakończenia
      2.5.4. liczbę jednoczesnych spotkań
3. Portal e-Urząd nie powinien umożliwiać dokonywania rezerwacji w dni wolne od pracy.
4. Portal e-Urząd powinien uprawniać pracownika urzędu do zarządzania zgłoszonymi wizytami przez Użytkownika:
   4.1. Potwierdzić termin wizyty,
   4.2. Zmienić termin wizyty,
   4.3. Odrzucić wizytę
5. Administrator/uprawniony pracownik musi mieć możliwość podglądu obciążenia/obłożenia kolejek w formie raportu.
6. Administrator powinien mieć możliwość personalizowania strony służącej do rezerwacji.
7. Portal e-Urząd powinien wysyłać powiadomienie e-mail do pracownika urzędu zarządzającego kalendarzem wizyt o wszelkich zgłoszeniach wizyt, lub zmianach w umówionej wizycie w zarządzanym przez niego kalendarzu.

XI. Konsultacje Społeczne

1. Portal e-Urząd powinien umożliwiać przeprowadzanie złożonego procesu konsultacji społecznych, składającego się z jednego lub wielu etapów i zróżnicowanych form w ramach jednej konsultacji społecznej.
2. Administrator lub inna osoba posiadająca odpowiednie uprawnienia dodaje też informację o kategoriach do jakich należy konsultacja. Kategorie spośród których może wybierać to: Inwestycje, Sprawy społeczne, sprawy sołectw, Sport, Edukacja, Zdrowie, Infrastruktura, Wydarzenia gminne, Planowanie przestrzenne.
3. Portal e-Urząd powinien umożliwiać zaprojektowanie harmonogramu przebiegu konsultacji – terminów rozpoczęcia i zakończenia konsultacji, każdego z jej etapów, jego form, przy czym musi umożliwiać takie zaprojektowanie harmonogramu, żeby można było uwzględnić również te formy konsultacji, dla których system nie przewiduje wsparcia. Harmonogram musi być jednocześnie mechanizmem kontrolującym przebieg konsultacji, który w sposób automatyczny odpowiednio włącza lub wyłącza dostęp do aktualnego etapu konsultacji. Harmonogram działa niezależnie dla każdej konsultacji i stanowi jej integralną część.
4. Portal e-Urząd powinien umożliwiać publikowanie wyników ankiety po zakończeniu konsultacji, jak również po jej zakończeniu oraz dodatkowo, po jej zakończeniu generować wyniki w postaci raportu.
5. Portal e-Urząd powinien prezentować statystki dotyczące poszczególnych konsultacji społecznych, czy jej etapów, w szczególności liczbę wypowiedzi lub oddanych głosów.
6. Portal e-Urząd powinien umożliwiać prowadzenie konsultacji w minimum następujących formach: ankiety, forum dyskusyjnego oraz opiniowania dokumentu.
7. **Ankieta:**
    - 7.1. może składać się z jednego lub wielu pytań, przy czym system nie może ograniczać ich maksymalnej liczby
    - 7.2. musi pozwalać na definiowanie pytań, dla których odpowiedź może stanowić:
        - 7.2.1. Tekst otwarty,
        - 7.2.2. Datę,
        - 7.2.3. Liczbę,
        - 7.2.4. Wskazanie pozycji na liście jednokrotnego wyboru,
        - 7.2.5. Wskazanie pozycji na liście jednokrotnego wyboru z otwartą możliwością wprowadzenia tekstu,
        - 7.2.6. Wskazanie pozycji na liście jednokrotnego wyboru z komentarzami,
        - 7.2.7. Wskazanie pozycji na liście wielokrotnego wyboru,
        - 7.2.8. Wskazanie pozycji na liście wielokrotnego wyboru z otwartą możliwością wprowadzenia tekstu,
        - 7.2.9. Wskazanie pozycji na liście wielokrotnego wyboru z komentarzami,
        - 7.2.10. Ranking dostępnych opcji – ułożenie ich w odpowiedniej kolejności,
        - 7.2.11. Macierz opcji i wartości.
8. do tworzenia ankiet system musi zapewniać odpowiedni kreator,
9. kreator musi umożliwiać tworzenie ankiet składających się z dowolnej liczby pytań i dowolnej liczby odpowiedzi dla każdego pytania,
10. może być wykorzystana jednokrotnie,
11. utworzona ankieta może być modyfikowana,
12. udział w ankiecie w danej konsultacji możliwy jest tylko jeden raz przez zalogowanego uczestnika.
13. **forum dyskusyjne:**
    - 13.1. może mieć jeden lub wiele poruszanych tematów, przy czym Portal nie może ograniczać maksymalnej liczby tematów,
    - 13.2. do tworzenia for dyskusyjnych system musi zapewniać odpowiedni kreator,
    - 13.3. Portal musi zapewniać możliwość wypowiadania się uprawnionym użytkownikom, a także musi zapewniać możliwość udzielania odpowiedzi innym użytkownikom, przy czym o możliwości tej

każdorazowo, w ramach parametrów konsultacji społecznej, decydować musi administrator konsultacji społecznej,

13.4. system musi zapewniać możliwość udzielania głosu poparcia w postaci polubienia (Tak lub Nie), przy czym o możliwości tej każdorazowo, w ramach parametrów konsultacji społecznej, decydować musi administrator konsultacji społecznej,

13.5. system musi zapewniać możliwość jednokrotnej lub wielokrotnej wypowiedzi na forum, w zależności od ustawień konsultacji społecznej,

13.6. system musi zapewniać możliwość rejestracji załączników dołączonych do opinii, przy czym o możliwości tej każdorazowo, w ramach parametrów konsultacji społecznej, decydować musi administrator konsultacji społecznej,

13.7. system musi udostępniać parametr, od którego zależeć będzie, czy opinia na forum pojawi się natychmiast, czy po zatwierdzeniu jej przez moderatora,

13.8. system musi umożliwiać przydzielenie moderatora dyskusji każdemu tematowi forum dyskusyjnego,

13.9. system musi umożliwiać administratorowi konsultacji odniesienie się do opinii wyrażonej na forum przez jego uczestnika.

14. **opiniowanie treści dokumentu:**

14.1. system musi umożliwiać prowadzenie konsultacji społecznej dowolnego dokumentu,

14.2. do tworzenia struktury konsultowanego dokumentu system musi zapewniać odpowiedni kreator,

14.3. system musi umożliwiać odwzorowanie struktury konsultowanego dokumentu w postaci elektronicznej według określonych wzorców i dać możliwość odniesienia się uczestnikom konsultacji do każdego z nich, przy czym uczestnik konsultacji musi mieć możliwość wyboru, z listy dostępnych odnośników/oznaczeń, fragmentu dokumentu, do którego wyraża swoją opinię np. paragraf, rozdział itp.,

15. Ekran danej konsultacji przygotowywany jest przez pracownika Urzędu, który przy tworzeniu konsultacji ma do wyboru metody konsultacyjne takie jak: dyskusja o dokumentach, mapa interaktywna, badanie ankietowe, wywiad indywidualny, sondaż, grupa dyskusyjna

16. Konsultacje społeczne muszą posiadać możliwość tworzenia szablonów które administrator może dowolnie modyfikować.

17. Konsultacje społeczne dodane w portalu muszą być również dostępne i możliwe do konsultowania z poziomu aplikacji mobilnej.

XII. Raporty

1. Portal e-Urząd umożliwia wydruk następujących raportów:
   1.1. rejestracji użytkowników z możliwością zawężenia na okres od-do.
   1.2. działania usług publicznych udostępnionych online,
   1.3. Raportowanie dot. statystyk w zakresie wizyt umówionych w urzędzie z poziomu modułu raportów
2. Portal e-Urząd w wydruku uwzględnia zastosowane filtry.

XIII. Pomoc

1. Portal e-Urząd powinien posiadać instrukcję obsługi Panelu Administratora w zakładce Pomoc.

Obsługa kont użytkowników

I. Rejestracja

1. Rejestracja nowego użytkownika odbywa się automatycznie podczas pierwszego logowania za pomocą Krajowego Węzła Tożsamości (KWT).
2. Przy pierwszym logowaniu użytkownik musi być zobowiązany do akceptacji regulaminu Systemu e-Urząd oraz mieć możliwość zapoznania się z jego treścią.
3. Dane do rejestracji (imię, nazwisko, PESEL) System e-Urząd automatycznie pobiera z Profilu Zaufanego.
4. Użytkownik musi dodatkowo wypełnić pole z adresem mailowym, po akceptacji regulaminu, regulamin w formacie PDF jest wysyłany na podany adres Użytkownika.

5. Użytkownicy powinni być informowani z wyprzedaniem o aspektach związanych z przetwarzaniem ich danych osobowych.
6. Po każdej aktualizacji regulaminu, użytkownik jest proszony o akceptację kolejnej wersji regulaminu.
7. Akceptacja regulaminu w Portalu, powinna mieć skutek w aplikacji mobilnej i na odwrót.

II. Logowanie

1. Portal e-Urząd powinien umożliwiać logowanie się za pomocą usługi SSO (Single Sign-On – pojedyncze logowanie) dostępnej w ramach KWT na https://login.gov.pl.
2. Portal e-Urząd powinien rejestrować wszystkie próby logowania oraz gromadzi i przechowuje następujące informacje: pełną datę i godzinę, nazwę konta, które zostało poddane uwierzytelnianiu, adres IP, z którego wykonane było uwierzytelnianie, rezultat uwierzytelniania (powodzenie/niepowodzenie).

III. Uprawnienia konta

1. Każdy użytkownik, który będzie chciał uzyskać dostęp do danych z systemów dziedzinowych, będzie musiał uwierzytelnić się za pomocą KWT – dane (imię, nazwisko i PESEL) pobierane są automatycznie.
2. Każdy użytkownik widzi i modyfikuje tylko swoje dane – dane osobowe oraz dane adresowe, formularze.
3. Modyfikacja PESELu, imienia oraz nazwiska nie jest możliwa przez użytkownika. PESEL pobierany jest tylko z KWT za pomocą API.
4. Każdy użytkownik może zarządzać swoim kontem w zakresie: wprowadzanie i zmiana danych osobowych (dane będą wykorzystane do automatycznego wypełnienia pól formularzy wniosków), wprowadzanie i zmiana adresu poczty elektronicznej, wyboru i zmiany tematyki otrzymywanych powiadomień.

IV. Konta firmowe

1. Dostęp do **Konta Firmowego (KF)** powinien odbywać się przez konto osoby fizycznej.
2. Dostęp do KF przez osobę fizyczną powinien być możliwy tylko po wcześniejszym złożeniu przez osobę do tego uprawnioną (osobę zarejestrowaną w Krajowym Rejestrze Sądowym danej osoby prawnej, lub osobę przez nią upoważnioną) wniosku **Upoważnienia do Konta Firmowego (UKF)**.
3. Nadanie UKF
   - 3.1. UKF dostępne jest jako e-usługa w Portalu e-Urząd,
   - 3.2. UKF pobiera dane:
     - 3.2.1. Firmy z bazy REGON na podstawie numeru REGON lub NIP,
     - 3.2.2. Wnioskodawcy od dostawcy tożsamości, za pośrednictwem którego zalogował się do Portalu,
   - 3.3. UKF jest podpisywany podpisem zaufanym lub podpisem kwalifikowanym elektronicznym, a następnie wysyłany na ePUAP urzędu.
   - 3.4. UKF wydawane jest tylko przez i dla osób fizycznych posiadających konto w Systemie e-Urząd oraz Profil Zaufany lub podpis kwalifikowany elektroniczny.
   - 3.5. UKF jest bezterminowe.
   - 3.6. Samo złożenie wniosku UKF nie daje upoważnionej osobie dostępu do KF.
   - 3.7. UKF jest zatwierdzane przez pracownika Urzędu po wcześniejszej weryfikacji danych faktycznych – sprawdzenie, czy wnioskodawca jest osobą uprawnioną do składania takich wniosków (weryfikacja w REGON /KRS).
4. Dostęp do KF powinien być możliwy po prawidłowym zalogowaniu się i wybraniu odpowiedniego profilu/kontekstu.
5. Osoba fizyczna, która uzyskała dostęp do KF na podstawie złożonego UKF (Wnioskodawca), powinna mieć możliwość nadawania dostępu do KF innym osobom fizycznym, bez potrzeby wysyłania kolejnych UKF. Wnioskodawca powinien mieć możliwość nadawania dostępu do poszczególnych modułów, tj. Korespondencji, zarządzania uprawnieniami, dostępu do danych podatkowych firmy.
6. Osoba fizyczna, która otrzymała dostęp do KF od Wnioskodawcy, musi otrzymać powiadomienie e-mail.

7. Osoba fizyczna zalogowana na KF musi widzieć dane (złożone wnioski, płatności, dane z systemów dziedzinowych) firmy – dane osoby fizycznej i firmy nie mieszają się.
8. Jedna osoba fizyczna może mieć dostęp do wielu KF.
9. System musi wyświetlać informacje danej firmy, w zakresie
   9.1. Nazwa Firmy
   9.2. Regon
   9.3. KRS
   9.4. NIP
   9.5. Dane adresowe siedziby
   9.6. Dane Wnioskodawcy (imię, nazwisko, pesel, skrytka ePUAP)
   9.7. Dane osoby upoważnionej (imię, nazwisko, pesel, skrytka ePUAP, rodzaj dostępu do poszczególnych modułów KF)
10. Użytkownicy, którzy otrzymali dostęp do KF w portalu, powinni mieć również dostęp do tego KF z poziomu aplikacji mobilnej.

V. Ułatwienia Dostępu

Z zakładki ułatwienia dostępu użytkownik może zmienić kolor oraz kontrast ekranów portalu wybierając jedną z pięciu opcji: podstawowy (WCAG 2.1), czarno-żółty, szaro-szary, niebiesko-biały, czarno-biały lub pozostać przy standardowym widoku Portalu. Po wyborze koloru użytkownik ma możliwość wybrania wielkości liter wyświetlanych w aplikacji, może wybrać wielkość: standardową, średnią i dużą.

VI. Katalogi

Po zalogowaniu użytkownik powinien mieć do wyboru w menu następujące zakładki:

1. **Moje płatności** – lista zobowiązań danego Użytkownika wraz z możliwością dodania ich do koszyka i dokonania płatności.
2. **Odebrane** – lista dokumentów otrzymanych od Urzędu:
   2.1. Użytkownik ma możliwość przeglądania tych dokumentów XML sformatowanych za pomocą stylu (ze wzoru z CRWDE), do którego ten dokument się odwołuje – taka możliwość istnieje również wtedy, kiedy styl nie jest dostępny bezpośrednio z CRWDE.
   2.2. Dokumenty te mogą być dostępne: po otrzymaniu przez Urząd podpisanej przez Użytkownika za pomocą Profilu Zaufanego zwrotki dostępnej z poziomu ESP; po upływie 14 od wysłania dokumentu do Użytkownika.
3. **Wysłane** – lista dokumentów XML wysyłanych do Urzędu za pośrednictwem portalu lub aplikacji mobilnej wraz z Urzędowym Poświadczeniem Przedłożenia (UPP) otrzymanym od ESP; Użytkownik ma możliwość przeglądania tych dokumentów XML sformatowanych za pomocą stylu (ze wzoru z CRWDE), do którego ten dokument się odwołuje – taka możliwość istnieje również wtedy, kiedy styl nie jest dostępny bezpośrednio z CRWDE.
4. **Robocze** – lista dokumentów (dostępne przez formularze xforms) częściowo wypełnionych i jeszcze nie wysłanych do Urzędu; Użytkownik ma możliwość powrotu do edycji w późniejszym czasie.
5. **e-Usługi** – lista wszystkich dostępnych e-usług z podziałem na kategorie. Użytkownik może wybrać dowolną i rozpocząć wprowadzanie danych.
6. **Podatki i opłaty lokalne** – wyświetlane są podatki i opłaty dotyczące danego Użytkownika w podziale na kategorie opłat.
7. **Umawianie Wizyt** – Lista dostępnych kalendarzy, gdzie Użytkownik może zgłosić umówienie wizyty w Urzędzie.
8. **Konsultacje Społeczne** – Lista wszystkich opublikowanych, konsultowanych, zakończonych i archiwalnych konsultacji społecznych prowadzonych przez Urząd. Miejsce, w którym Użytkownik może wziąć udział w konsultacji lub sam zgłosić własną konsultację.
9. **Powiadomienia** – Lista wszystkich dostępnych powiadomień, które użytkownik może otrzymać po wyrażeniu zgody na doręczenie i oznaczenie kanału wysyłki.

10. **Moje dane** – dane dotyczące zalogowanego Użytkownika.
11. **Pomoc** – instrukcja obsługi Systemu e-Urząd.

VII. Komunikacja z Urzędem

Użytkownik – Urząd:

1. Wszystkie dokumenty tworzone przez Użytkownika w Portalu e-Urząd są wysyłane do Urzędu przez ESP, a ich odebranie potwierdzone jest za pomocą UPP.

Wysłanie dokumentu do Urzędu

2. Użytkownik wybiera usługę.
3. Portal e-Urząd automatycznie wypełnia danymi pola w formularzu:
   3.1. Imię, Nazwisko i numer Pesel są pobierane od dostawcy tożsamości za pośrednictwem, którego Użytkownik logował się do Portalu,
   3.2. Dane dotyczące adresu, numeru telefonu i e-mail są pobierane z 'Moich danych', jeśli Użytkownik je wcześniej uzupełnił i zapisał.
4. Użytkownik uzupełnia pozostałe dane.
5. Portal e-Urząd sprawdza dokument pod kątem zgodności ze schematem (xsd) dostępnym CRWDE (ta czynność dostępna jest również przy braku komunikacji z https://crd.gov.pl)
6. Jeśli usługa wymaga płatności, to Użytkownik, jest kierowany do systemu transakcyjnego umożliwiającego dokonanie płatności.
7. Informacja o płatności dołączana jest do dokumentu w taki sposób, żeby pracownicy Urzędu mogli jednoznaczne wskazać tę płatność na liście przychodów na rachunku Urzędu.
8. Użytkownik podpisuje dokument za pomocą Podpisu Zaufanego.
9. Użytkownik gotowy dokument wysyła na ESP Urzędu.
10. Portal e-Urząd w zależności od typu dokumentu kieruje dokument na różną skrytkę (jeśli Administrator ustawi różne skrytki do typów dokumentów).
11. Użytkownik zaraz po wysłaniu dokumentu otrzymuje UPP.
12. Formularz, który został częściowo uzupełniony i nie został wysłany, powinien być dostępny dla Użytkownika w pismach roboczych, z takim stanem uzupełnienia, w jakim go zostawił.

Urząd – Użytkownik

13. Portal e-Urząd udostępnia e-usługę, za pomocą której, Użytkownik będzie mógł wyrazić Zgodę na Otrzymywanie Korespondencji w Formie Elektronicznej (ZOKFE) od Urzędu.
14. Użytkownik musi mieć wgląd do aktualnej i historycznej informacji o wysłanych ZOKFE.
15. ZOKFE wysłane z poziomu portalu powinno być dostępne w aplikacji mobilnej i na odwrót.

Wysyłanie dokumentu do Użytkownika

16. Dokument XML generowany jest w obiegu dokumentów EZD.
17. Dokument jest podpisywany za pomocą podpisu zaufanego lub podpisu kwalifikowanego elektronicznego.
18. Portal e-Urząd wysyła dokument do Użytkownika przez e-PUAP.
19. Użytkownik podpisuje Urzędowe Poświadczenie Doręczenia (UPD) i dopiero wtedy ma dostęp do dokumentu.
20. UPD wraca do systemu EZD i dokument otrzymuje status "dostarczony".
21. Od tego momentu ten sam dokument jest widoczny również w Portalu e-Urząd i jest wyświetlany z wykorzystaniem stylu umieszczonego w CRWDE. Portal e-Urząd ma zapewnić prawidłowe wyświetlanie dokumentów również w sytuacji, kiedy CRWDE nie jest dostępne.
22. Dokumenty wysłane z portalu mają być widoczne w aplikacji mobilnej i na odwrót.

e-Usługi

23. Każdy zalogowany Użytkownik powinien mieć dostęp do wszystkich dostępnych (opublikowanych) e-usług.

24. Portal e-Urząd powinien być wyposażony w ESP udostępnioną na ePUAP.
25. Wszystkie formularze powinny posiadać ustandaryzowaną strukturę – nagłówek, treść, stopka.
26. Wysłanie dokumentu do urzędu (dokument stworzony na podstawie wypełnionego formularza) powinno być potwierdzone za pomocą UPP.
27. Formularz każdej e-usługi powinien być wykonany w technologii XForms i wykonywany przez aplikację typu server-side.
28. Formularze powinny zapewniać poprawność i kompletność danych wprowadzanych poprzez:
    28.1. Portal e-Urząd automatycznie wypełnia pola w formularzu:
        28.1.1. Danymi pobieranymi od dostawcy tożsamości, tj. imię, nazwisko oraz numer pesel,
        28.1.2. danymi dostępnymi w profilu Użytkownika, jeśli je uzupełnił, tj. . adres zamieszkania lub adres korespondencyjny, numer telefonu oraz e-mail.
    28.2. Portal e-Urząd automatycznie wypełnia danymi pola formularza w przypadku, jeśli taki sam formularz został wcześniej wysłany do Urzędu – raz prawidłowo wprowadzone dane kopiują się do kolejnych podobnych (opcja *Wyślij ponownie*).
    28.3. Portal e-Urząd pozwala wysłać dokument tylko wtedy, kiedy wszystkie wymagane dane zostaną wprowadzone i te dane będą poprawne, w przeciwnym wypadku Portal e-Urząd wyświetli Użytkownikowi odpowiedni komunikat.
    28.4. Formularze powinny posiadać mechanizmy:
        28.4.1. walidacja PESELu, NIPu;
        28.4.2. ukrywanie/pokazywanie poszczególnych pól w zależności od wyborów (np. pola do wprowadzenia adresu korespondencyjnego innego niż zameldowania);
        28.4.3. załączania plików;
        28.4.4. automatycznego uzupełniania danych teleadresowych, jeśli zostały uzupełnione w koncie użytkownika;
        28.4.5. walidacji z bazą TERYT oraz PNA
        28.4.6. Pobierania stawek podatkowych (dotyczy deklaracji oraz informacji podatkowych).

Podpisywanie

29. Podpisywanie dokumentu powinno być dostępne jako integralny etap w procesie wysyłania dokumentu do Urzędu.
30. Podpisywanie powinno odbywać się za pomocą podpisu elektronicznego weryfikowanego przez e-PUAP (Podpis Zaufany).

Płatności

31. By zapewnić osobom fizycznym i prawnym możliwość opłacenia wybranych należności, należy wykorzystać system płatności internetowych PayByNet.
32. Zastosowany system płatności elektronicznych PayByNet powinien spełniać minimum następujące wymagania:
    32.1. obsługiwać popularne banki w Polsce,
    32.2. gwarantować dostępność środków na koncie wysyłającego,
    32.3. umożliwia dołączenie własnej treści tytułu płatności.
33. Portal e-Urząd powinien umożliwiać opłacenie tych usług, które takiej opłaty wymagają.
34. Płatność za usługę powinna być dostępna jako integralny etap w procesie wysyłania dokumentu do Urzędu.
35. Użytkownik powinien widzieć tylko swoje płatności.
36. Informacje o płatnościach pobierane są za każdym razem z systemów dziedzinowych Urzędu.
37. Portal e-Urząd powinien wyświetlać wszystkie oczekujące płatności, czyli kwoty, które Użytkownik ma wnieść na rzecz Urzędu jako podatek lub opłata lokalna.
38. Portal e-Urząd powinien umożliwiać wniesienie tylko części wybranej opłaty.
39. Portal e-Urząd powinien umożliwiać wniesienie części opłaty (rat różnych opłat w jednej transakcji – np. 1-sza rata podatku od nieruchomości oraz 2-ga rata podatku rolnego, o ile są wnoszone na ten sam rachunek bankowy Urzędu).

40. Tytuł przelewu powinien jednoznacznie wskazywać, które opłaty i w jakich częściach zostały wniesione jako jeden transfer. Użytkownik ma możliwość dodania do tytułu przelewu nr faktury/decyzji.
41. Portal e-Urząd powinien wyświetlać Użytkownikowi płatności:
    41.1. wniesione za pomocą Systemu Transakcyjnego,
    41.2. nieudane próby wniesienia opłaty za pomocą Systemu Transakcyjnego.
42. Portal e-Urząd powinien posiadać możliwość automatycznego, zgodnego z zadanym harmonogramem, wysyłania powiadomień o zaległościach płatniczych do Użytkowników posiadających konto w Systemie e-Urząd.
43. Informacje o dokonanych wpłatach przez portal e-Urząd powinny się również wyświetlać w aplikacji mobilnej

VIII. Podatki i opłaty

1. Użytkownik powinien widzieć informację tylko o swoich podatkach i opłatach.
2. Informacje o podatkach i opłatach muszą być pobierane z systemów dziedzinowych Urzędu.
3. System e-Urząd powinien umożliwiać wyświetlanie minimum następujących danych:
    3.1. Informacje o podatkach od nieruchomości
    3.2. Informacje o podatku rolnym
    3.3. Informacje o podatku rolnym
4. Podatki od gruntów i nieruchomości – system powinien wyświetlać nieruchomości na mapie geograficznej.

IX. Konsultacje społeczne

1. Dostęp do danych i funkcjonalności oferowanych w ramach Portalu e-Urząd jest zapewniony dla:
    1.1. Użytkowników publicznych (jeśli Administrator tak zdefiniuje)– nie posiadają konta i mają dostęp jedynie w zakresie przeglądania konsultacji i publicznej treści Systemu e-Urząd.
    1.2. Użytkowników zalogowanych – mają możliwość zgłoszenia konsultacji i udziału w konsultacjach, korzystania z innych e-Usług.
2. Portal powinien umożliwiać prowadzenie konsultacji społecznych z mieszkańcami, organizacjami, stowarzyszeniami i jednostkami własnymi JST, obejmujące swoim zasięgiem obszar działania urzędu lub wybrane jego części w formie: forum dyskusyjnego i/lub ankiet i/lub konsultacji dokumentu.
3. Portal e-Urząd ma umożliwiać Użytkownikom branie udziału w konsultacjach społecznych dotyczących następujących obszarów:
    - uchwalania miejscowego planu zagospodarowania przestrzennego,
    - zmiany granic gmin lub miasta,
    - tworzenia programów współpracy miast z organizacjami pozarządowymi,
    - ocen oddziaływania inwestycji na środowisko,
    - w każdej innej sytuacji, w które urząd chce poznać zdanie mieszkańców.
4. Użytkownik może zapoznać się z konsultacjami aktualnie prowadzonymi, jeszcze nie rozpoczętymi oraz zakończonymi. Użytkownik może również wyszukać interesujące go konsultacje dzięki wykorzystaniu słownej wyszukiwarki np. poprzez wpisanie fragmentu jej tytułu lub wybraniu kategorii konsultacji, statusu konsultacji, daty publikacji konsultacji (zakres od do) lub typu konsultacji .
5. Użytkownik może wyszukać konsultacji również używając kalendarza konsultacji. Z kalendarza konsultacji użytkownik może przejść do szczegółów konsultacji.
6. Konsultacje mogą posiadać status:
    - Opublikowana
    - Konsultowana
    - Zakończona
    - Archiwalna
7. Użytkownik może zobaczyć status na liście konsultacji.
8. Zakres danych formularza zgłoszenia projektu konsultacji obejmuje:
    8.1. Tytuł – pole tekstowe (obligatoryjne)

8.2. Opis – pole tekstowe z wykorzystaniem edytora WYSYWIG (obligatoryjne)
8.3. Uzasadnienie – pole tekstowe z wykorzystaniem edytora WYSYWIG (obligatoryjne)
8.4. Lokalizacja - lokalizacja związana z zgłoszoną konsultacją (opcjonalne):
8.5. Dane zgłaszającego (rodzaj zgłaszającego: pole wyboru: osoba fizyczna, podmiot)
8.6. Kategoria – pole słownikowe: Inwestycje, Sprawy społeczne, Sprawy sołectw, Sport, Edukacja, Zdrowie, Infrastruktura, Wydarzenia gminne, Planowanie przestrzenne, Inne.
8.7. Rodzaj - pole wybory z słownika: opiniowanie dokumentu, ankieta, grupa dyskusyjna. W zależności od wybranego rodzaju formularz prezentuje dodatkowe sekcji:

9. Przy zakończonych konsultacjach Użytkownik może zobaczyć datę zakończenia konsultacji oraz przeglądać sprawozdanie z konsultacji. Przy jeszcze nierozpoczętych konsultacjach użytkownik widzi datę rozpoczęcia konsultacji. Przy konsultacjach w trakcie trwania użytkownik widzi czas trwania konsultacji.
10. System powinien umożliwiać automatyczne powiadamianie zarejestrowanych osób, które wyraziły chęć otrzymywania powiadomień o zbliżających się terminach konsultacji lub ich etapów (PUSH lub e-mail).

X. Umawianie Wizyt

1. Portal e-Urząd ma umożliwić umówienie wizyty Użytkownika w Urzędzie.
2. Usługa jest dostępna dla Użytkowników zalogowanych oraz niezalogowanych.
3. Użytkownik Portalu umawia wizytę w urzędzie poprzez:
   3.1. prawidłowe wypełnienie zgłoszenia w module umawiania wizyt w Portalu,
   3.2. zatwierdzenie wprowadzonych danych,
4. Użytkownik przy umawianiu wizyty musi:
   4.1. Wybrać komórkę organizacyjną, w której chce umówić wizytę,
   4.2. Wybrać wolny termin wizyty z widoku kalendarza,
   4.3. Uzupełnić szczegóły wizyty, w tym podaje:
      4.3.1. cel wizyty,
      4.3.2. numer telefonu (o ile zdefiniowany kalendarz ma tę opcję włączoną) – w celu otrzymania potwierdzenia umówienia wizyty bądź ewentualnego kontaktu ze strony Urzędu,
      4.3.3. adres e-mail (o ile zdefiniowany kalendarz ma tę opcję włączoną) – w celu otrzymania potwierdzenia umówienia wizyty bądź ewentualnego kontaktu ze strony Urzędu,
      4.3.4. swój adres zamieszkania (nieobligatoryjne).
5. Po umówieniu wizyty, na podany adres e-mail zostanie wysłana wiadomość z potwierdzeniem rejestracji wizyty.

XI. Pomoc

1. Portal e-Urząd powinien posiadać instrukcję obsługi Użytkowania Portalu e-Urząd w zakładce Pomoc.

Wymagania niefunkcjonalne e-Urząd

167. System e-Urząd powinien być zbudowany w architekturze trójwarstwowej. Rozdzielone są: warstwa prezentacji, logiki biznesowej oraz bazy danych.
168. Interfejs Systemu e-Urząd powinien być dostępny za pomocą przeglądarki internetowej (Microsoft Edge, Firefox, Chrome, Safari w najnowszych wersjach) pracującej w dowolnym systemie operacyjnym (MS Windows, Linux oraz Mac OS X), jeśli dana przeglądarka jest dostępna dla danego systemu operacyjnego.
169. System e-Urząd powinien posiadać interfejsy komunikacyjne w postaci usług sieciowych.
170. Interfejsy komunikacyjne Systemu e-Urząd będą oparte na standardach SOAP, WSDL i XML lub HTTP zgodne z REST.
171. System e-Urząd działa z wykorzystaniem tzw. przyjaznych adresów internetowych.
172. System e-Urząd działa w oparciu o kodowanie UTF-8.
173. System e-Urząd powinien być uruchomiany jest w hostingu udostępnianym przez Usługodawcę.

174. Aspekty Bezpieczeństwa:
    174.1. System e-Urząd powinien posiadać możliwość tworzenia kopii bezpieczeństwa bazy danych. Dostarczone narzędzia powinny posiadać możliwość definiowania harmonogramów automatycznego wykonywania kopii. Kopie bezpieczeństwa zapewniają możliwość odzyskania danych i przywrócenia całego Systemu e-Urząd do stanu normalnej pracy po ewentualnej awarii sprzętowej lub programowej.
    174.2. System e-Urząd powinien być dostępny jest w całości dla użytkownika końcowego przez wykorzystanie protokołu SSL (HTTPS).
    174.3. System e-Urząd musi być odporny jest na ataki typu Cross-site scripting (XSS) i Cross-site request forgery (XSRF).

APLIKACJA MOBILNA

Informacje Ogólne

Niniejszy dokument stanowi opis wymagań dla aplikacji mobilnej funkcjonującej w ramach zintegrowanego systemu e-Urząd. Dokumentacja będzie podstawą do odbioru systemu.

Aplikacja mobilna jest bezpłatna dla użytkownika końcowego, dostępna w wersji na telefon i tablet z systemem operacyjnym Android oraz iOS. Głównym celem aplikacji jest dostarczenie obywatelom i przedsiębiorcom bezpiecznego dostępu do danych z Rejestrów Publicznych, a także sprawnej komunikacji z JST.

Celem wdrożenie aplikacji mobilnej jest ułatwienie kontaktu obywateli i przedsiębiorców z administracją publiczną. Ze względu na zwiększone wykorzystanie technologii mobilnych, a także rosnącej dostępności publicznej informacji, danych i usług internetowych, usługi publiczne muszą być świadczone nowymi kanałami.

Wymagania Funkcjonalne Aplikacji

175. Dostarczona aplikacja musi być pełnoprawną aplikacją natywną dostarczoną na system Android i iOS. Przygotowanie i przetwarzanie danych odbywa się bezpośrednio w aplikacji. Aplikacja komunikuje się z serwerem w celu zapisu oraz odczytu danych.
176. Aplikacja mobilna musi być zintegrowana z portalem e-Urząd oraz systemem EZD.
177. Z poziomu aplikacji mobilnej Użytkownik powinien mieć dostęp do zasobów Gminy oraz innych jednostek organizacyjnych bez konieczności instalowania oddzielnych aplikacji. Po zalogowaniu do aplikacji za pomocą kodu PIN lub biometrii Użytkownik może wybrać, do zasobów jakiej jednostki wchodzi.
178. Użytkownik może wybrać domyślną jednostkę, która będzie uruchamiała się po włączeniu aplikacji lub dodać ją do ulubionych. Po ponownym wejściu do aplikacji użytkownik będzie widział ostatnią gminę, w obrębie której się poruszał lub domyślną gminę, którą ma możliwość wybrania z poziomu ustawień aplikacji.
179. Przy pierwszym uruchomieniu aplikacji musi być sprawdzenie, czy aplikacja ma dostęp do platformy e-Urząd.
180. Użytkownik końcowy aplikacji ma możliwość korzystania z 2 profili aplikacji – osoby fizycznej lub profilu firmowego.
181. Użytkownik może z poziomu aplikacji mobilnej nadać uprawnienia do profilu firmowego dla przedsiębiorcy lub osoby uprawnionej.
182. Użytkownik powinien mieć możliwość logowania do aplikacji za pomocą kodu PIN lub biometrii (odcisk palca, rozpoznawanie twarzy). Bez nadania kodu PIN nie można zobaczyć jej zawartości.
183. Biometria jest wykorzystywana zamiennie z kodem PIN, lecz nie może w odróżnieniu od kodu PIN występować samodzielnie.
184. Użytkownik ma opcję zmiany jednostki, w ramach kontekstu której się porusza. Po przejściu do nieuwierzytelnionej wcześniej jednostki użytkownik musi potwierdzić swoją tożsamość za pomocą KWT. Użytkownik posiada jeden kod PIN do wielu jednostek. Kod PIN jest związany z urządzeniem mobilnym na którym jest nadawany i służy do autoryzacji tylko na tym konkretnym urządzeniu.

185. Podczas pierwszego logowania do aplikacji użytkownik musi zatwierdzić regulamin. Podczas każdego następnego logowania następuje weryfikacja, czy użytkownik zatwierdził już aktualny regulamin, ponieważ regulamin może ulec zmianie. Jeśli nie zatwierdził nowego regulaminu to zostaje o to poproszony.
186. Dostęp do zasobów aplikacji odbywa się w dwóch trybach: dla użytkowników nieuwierzytelnionych – jedynie nadanie kodu PIN (mogą przeglądać funkcjonalności aplikacji, widzą listę konsultacji dla nieuwierzytelnionych użytkowników, widzą listę e-usług); dla użytkowników uwierzytelnionych – za pomocą KWT (mogą korzystać w pełni z funkcjonalności aplikacji: wypełniać i wysyłać e-usługi, wysyłać konsultacje społeczne, widzieć swoje informacje podatkowe i uiszczać opłaty za zobowiązania, otrzymywać powiadomienia).
187. Po zautoryzowaniu użytkownika w aplikacji mobilnej poprzez KWT zostaje również założone lub połączone konto na portalu e-Urząd.
188. W przypadku zapomnienia kodu PIN, użytkownik ma możliwość ponownego uwierzytelnienia za pomocą KWT, by odzyskać dostęp do aplikacji.
189. Uwierzytelnienie za pomocą KWT powinno odbywać się w webview aplikacji mobilnej, bez przekierowania do przeglądarki na urządzeniu mobilnym. Po prawidłowym uwierzytelnieniu użytkownik może korzystać w pełni z aplikacji, logując się do niej za pomocą kodu PIN.
190. Aplikacja musi umożliwiać zmianę kodu PIN wykorzystywanego do logowania do aplikacji.
191. Aplikacja musi być wyposażona w wyszukiwarkę globalną umożliwiającą w łatwy sposób wyszukanie treści w aplikacji.
192. Z poziomu aplikacji mobilnej użytkownik powinien mieć możliwość zgłoszenia propozycji konsultacji społecznej, pismo zostaje dostarczone na skrytkę ePUAP Urzędu po wcześniejszym podpisaniu zgłoszenia podpisem zaufanym. Użytkownik ma dostęp do wysłanego zgłoszenia i wystawionego UPP z poziomu skrzynki nadawczej.
193. Użytkownik powinien mieć możliwość przeglądania ogłoszonych konsultacji społecznych w formie listy lub w formie wydarzeń w kalendarzu. Użytkownik może wykorzystać filtry, aby wyszukać konsultacje np. w danej kategorii czy w danym statusie.
194. Użytkownik, aby wziąć udział w konsultacji społecznej musi się uwierzytelnić za pomocą KWT.
195. Aplikacja powinna umożliwiać Użytkownikowi przeglądanie konsultacji społecznych dla profilu prywatnego i firmowego, jednak, by wziąć udział w konsultacji musi przełączyć się na odpowiedni kontekst.
196. Użytkownik z poziomu aplikacji mobilnej powinien mieć możliwość wziąć udział w konsultacjach społecznych o różnym typie, min.: ankieta, opiniowanie dokumentu, forum dyskusyjne.
197. Użytkownik może przeglądać sprawozdania z konsultacji społecznych zakończonych.
198. Użytkownik może ustawić chęć otrzymywania powiadomień PUSH o konsultacjach, w których brał udział, o konsultacjach które sam zgłosił, o zmianach statusów konsultacji oraz przypomnienia o zbliżającym się terminie końcowym konsultacji lub przedłużeniu terminu konsultacji. Będą one generowane automatycznie.
199. Użytkownik z poziomu konsultacji społecznej ma dostęp do sprawozdania z zakończonej konsultacji.
200. Użytkownik ma dostęp do e-usług dostępnych w aplikacji mobilnej, minimum:
    - Upoważnienie do konta przedsiębiorcy
    - Pismo ogólne do podmiotu publicznego
    - Informacja o gruntach
    - Informacja o nieruchomościach i obiektach budowlanych
    - Informacja o lasach
    - Deklaracja na podatek rolny
    - Deklaracja na podatek od nieruchomości
    - Deklaracja na podatek leśny
    - Zgłoszenie konsultacji społecznej.
201. Użytkownik może wypełnić formularze e-usług podzielone na kilka kroków, co ułatwia ich wypełnienie.
202. Dokumenty oparte są o wzory opublikowane w CRWDE.

203. Użytkownik wypełniając formularz, ma dostęp do podpowiedzi, które sprawdzają poprawność wypełnianych danych takie jak: walidacja pól formularza - pola obowiązkowe, pomoc kontekstowa, sprawdzenie poprawności danych.
204. Dane zapisane na koncie użytkownika uzupełniają automatycznie formularze.
205. Użytkownik może zobaczyć kartę e-usługi, która pomoże mu poprawnie wypełnić formularz oraz poinformuje o dalszych krokach związanych z formularzem.
206. Wypełnione formularze zapisane zostają w wersjach roboczych dokumentów. Zapisane dokumenty dostępne są tylko na urządzeniu, na którym zostały wypełnione.
207. Wysyłanie pisma wykonywane jest w formie dokumentu elektronicznego na skrytkę gminy. Aby wysłać dokument użytkownik musi być zalogowany do aplikacji mobilnej oraz musi podpisać dokument za pomocą podpisu zaufanego.
208. Użytkownik może przeglądać wysłane dokumenty dostępne z poziomu skrzynki nadawczej, użytkownik może zobaczyć podgląd wypełnionego dokumentu. Z poziomu skrzynki nadawczej użytkownik może również pobrać dokument na urządzenie mobilne. Wysłane dokumenty dostępne są również z poziomu portalu e-Urząd.
209. Użytkownik może zobaczyć potwierdzenie nadania pisma z poziomu skrzynki nadawczej, może pobrać potwierdzenie dokumentu na urządzenie mobilne w formacie xml. Może zobaczyć również podgląd potwierdzenia dokumentu w formacie pdf.
210. Użytkownik może ponowić wysyłkę wysłanego dokumentu.
211. Użytkownik ma możliwość korzystania z bazy TERYT/PNA przy uzupełnianiu pól adresowych podczas wypełniania formularzy e-usług.
212. Użytkownik może korzystać z pomocy aplikacji w formie automatycznych wyliczeń wg obowiązujących stawek podatku podczas wypełniania e-usług deklaracji i informacji podatkowych.
213. Użytkownik może wysłać pismo ogólne na skrytki ePUAP do wielu podmiotów jednocześnie. Do każdego pisma użytkownik otrzymuje UPP.
214. Użytkownik może przeglądać pisma, które wysłał z poziomu skrzynki nadawczej. Pisma wysłane z poziomu aplikacji mobilnej są również dostępne w skrzynce nadawczej na portalu e-Urząd.
215. Odpowiedź na wysłane pismo użytkownik otrzyma do skrzynki odbiorczej na portalu e-Urząd.
216. Użytkownik z poziomu aplikacji mobilnej po uwierzytelnieniu KWT może przeglądać informacje o podstawie opodatkowania min. w kwestii podatku od nieruchomości, rolnego, leśnego. Informacje powinny być pobrane w czasie rzeczywistym z portalu e-Urząd.
217. Użytkownik może zwizualizować opodatkowane działki na mapie geograficznej.
218. Użytkownik ma dostęp do spersonalizowanej informacji o zobowiązaniach podatkowych (min. podatek od nieruchomości, rolny, leśny) z portalu e-Urząd, które dostępne są po uwierzytelnieniu za pomoc KWT.
219. Użytkownik może zobaczyć zestawienie płatności np. historię płatności, płatności, które musi wykonać, statusy płatności.
220. Użytkownik może dodać płatności do koszyka. Jedna pozycja może zostać dodana do koszyka tylko jeden raz. Użytkownik może wykonać płatność za pomocą zdefiniowanych na portalu e-Urząd pośredników płatności.
221. Użytkownik może sortować i filtrować płatności wg terminu płatności, kategorii zobowiązań, zakres kwot do opłacenia, dokonanych już wpłat, status transakcji.
222. Użytkownik może ustawić powiadomienia PUSH o zbliżającym się terminie płatności lub zaległości.
223. Użytkownik może uzupełnić dane w zakładce Moje dane z pomocą bazy TERYT/PNA, jeśli nie były wcześniej uzupełnione na platformie e-Urząd. Dane użytkownika są aktualizowane między aplikacją a portalem e-Urząd.
224. Użytkownik za pomocą aplikacji może złożyć oświadczenie w sprawie otrzymywania korespondencji drogą elektroniczną. Pismo jest wysyłane na skrytkę ePUAP Urzędu po podpisaniu go przez Użytkownika. Wyrażone zgody i rezygnacje muszą synchronizować się pomiędzy portalem e-Urząd, aplikacją i systemem obiegu dokumentów. Użytkownik musi zalogować się do aplikacji za pomocą KWT, aby złożyć oświadczenia.

225. Gmina może decydować, które z trzech dostępnych zgód będą widzieć jej użytkownicy: pisma administracyjne, decyzje podatkowe, faktury i rachunki – w zależności od ustawień w panelu administratora portalu e-Urząd.
226. Użytkownik może przeglądać wysłane oświadczenia z poziomu skrzynki nadawczej.
227. Użytkownik może wysłać oświadczenia do wielu jednostek jednocześnie, wybierając z listy do 5 jednostek.
228. Użytkownik może zmienić wygląd aplikacji dostosowując kolor, kontrast oraz wielkość liter w aplikacji.
229. Użytkownik może wybrać powiadomienia, które chce otrzymywać (w ramach kategorii zdefiniowanych przez administratora systemu na portalu e-Urząd). Dodatkowo może ustawić okres, po których powiadomienia będę usuwane, domyślnie będzie to 30 dni.
230. Z zakładki moje konto użytkownik ma dostęp do: ustawień aplikacji w tym ustawienia powiadomień oraz lista ulubionych gmin, domyślnej gminy, moich danych, oświadczeń, dostępie w tym zmiana kodu PIN, ustawienia bądź rezygnacji z biometrii oraz usunięcie danych aplikacji, usunięcia urządzenia, regulaminu aplikacji.
231. Z zakładki ułatwienia dostępu użytkownik może zmienić kolor oraz kontrast ekranów aplikacji wybierając jedną z pięciu opcji: podstawowy (WCAG 2.1), czarno-żółty, szaro-szary, niebiesko-biały, czarno-biały lub pozostać przy standardowym widoku aplikacji. Po wyborze koloru użytkownik ma możliwość wybrania wielkości liter wyświetlanych w aplikacji, może wybrać wielkość: standardową, średnią i dużą.
232. Z poziomu menu użytkownik ma również możliwość wylogowania się z aplikacji.
233. Dane osobowe i kontaktowe użytkownik uzupełnia oddzielnie dla każdego profilu – osoby fizycznej oraz podmiotu.

Wymagania Niefunkcjonalne Aplikacji

234. Aplikacja powinna działać na systemach od iOS 13.0 i Android 8.0.1.
235. Aplikacja powinna utrzymywać stałą, konsekwentną szatę graficzną i kolorystyczną - styl przycisków, czcionki, kolory, animacje.
236. Aplikacja będzie zgodna z Human Interface Guidelines (iOS) oraz Material Design Guidelines (Android).
237. Aplikacja powinna spełniać wytyczne standardu WCAG 2.1.
238. Interfejs aplikacji powinien w podstawowy sposób dopasowywać się do tabletów.
239. Aplikacja powinna mieć oddzielone warstwy - sieciową, widokową i biznesową.
240. Aplikacja powinna jawnie poprosić o uprawnienia do wysyłania powiadomień PUSH z czytelnym i prostym opisem.
241. Aplikacja powinna w bezpieczny sposób przechowywać wyliczony skrót kodu PIN.
242. Aplikacja powinna być napisana w sposób modułowy, co ułatwi wprowadzanie kolejnych zmian i nowych funkcjonalności (np. Moduł logowania, ekran główny, ekran powiadomień).
243. Funkcjonalności aplikacji, które nie wymagają uwierzytelnienia, powinny być dostępne w trybie offline.
244. Aplikacja powinna zbierać dane o urządzeniu oraz wersji systemu operacyjnego w celu lepszego wsparcia i wdrażania nowych funkcjonalności.
245. Aplikacja mobilna powinna posiadać dwa tryby aktualizacji
    - miękki - informacja, że jest nowa wersja aplikacji i należy dokonać aktualizacji przez Apple Store lub Google Play
    - twardy - komunikat w aplikacji, który blokuje korzystanie z aplikacji i wymusza aktualizację aplikacji. Krytyczne, gdy wdrażane są nowe funkcjonalności i zmiany, które nie są kompatybilne ze starszą wersję aplikacji.
246. Aspekty bezpieczeństwa:
    - dla aplikacji mobilnej należy uwzględnić wytyczne OWASP Mobile Top 10 - https://owasp.org/www-project-mobile-top-10/;
    - dla aplikacji serwerowej udostępniającej REST API należy uwzględnić wytyczne - https://owasp.org/www-project-api-security/;
    - W celu zapewnienia odpowiednich mechanizmów bezpieczeństwa zaleca się stosowanie dobrych praktyk opisanych w Application Security Verification Standard 4.0.2.

247. Aplikacja mobilna powinna być zintegrowanym elementem systemu e-Urząd (portal, system obiegu dokumentów eZD).

ELEKTRONICZNE ZARZĄDZANIE DOKUMENTACJĄ

WYMAGANIE MINIMALNE JAKIE MUSI ZAPEWNIĆ WYKONAWCA

Wymagania niefunkcjonalne EZD:

248. EZD musi posiadać architekturę trójwarstwową:
    a. warstwa prezentacji, obejmująca interfejsy użytkownika klienta WWW,
    b. warstwa aplikacji, obejmującą serwer Systemu,
    c. warstwa danych, zawierającą serwer bazy danych.
249. EZD musi umożliwiać pracę w trzech trybach:
    d. w trybie wspierającym obieg dokumentów papierowych
    e. w trybie EZD.
    f. w trybie mieszanym
250. Interfejs uużytkownika systemu musi być w całości polskojęzyczny. W języku polskim muszą być również wyświetlane wszystkie komunikaty przekazywane przez System, włącznie z komunikatami o błędach.
251. EZD musi informować użytkownika w momencie zaciągania plików, że plik przekroczył dopuszczalny rozmiar.
252. EZD musi przechowywać wszystkie dane w bazie danych zgodnej ze standardem SQL oraz zapewniającej transakcyjność operacji. Dopuszcza się przechowywanie poza bazą danych plików, w postaci repozytorium dyskowego – ich integralność z systemem musi być zapewniona przez metadane opisujące poszczególne pliki. Metadane muszą być przechowywane w bazie danych.
253. EZD musi działać w środowiskach systemowych bazujących na technologii Microsoft Windows oraz w środowiskach opartych na systemie Linux.
254. EZD musi umożliwiać dostęp do systemu przez użytkownika końcowego z poziomu przeglądarki internetowej, co najmniej Firefox, Google Chrome, MS Edge, Safari w najnowszych wersjach.
255. EZD musi cechować się interfejsem użytkownika opartym na nowoczesnych rozwiązaniach: wykorzystywać menu, listy, formularze, przyciski, referencje (linki), itp.
256. Wymaga się, aby interfejs użytkownika EZD stosował oznaczanie pól wymaganych na formularzu ekranowym w sposób wyróżniający te pola, a w przypadku ich błędnego wypełnienia jednoznacznie wskazywał na pola błędnie wypełnione.
257. EZD musi cechować duża elastyczność, rozumiana jako możliwość dostosowania systemu do zmieniających się wymagań funkcjonalnych wynikających ze zmieniającego się stanu prawnego i zmieniających się warunków praktycznych i przepisów prawnych.
258. EZD musi zabezpieczać dane przed przypadkowym nadpisaniem w przypadku równoczesnego korzystania z tych danych przez wielu użytkowników.
259. EZD musi posiadać widok indywidualny, prezentujący tylko te składniki systemu, do których uprawniony jest dany użytkownik.
260. System musi umożliwiać integrację z Active Directory w trybie SSO (Single Sign On). Logowanie do systemu odbywa się automatycznie za pomocą danych z konta AD. Użytkownik po zalogowaniu do AD nie musi logować się drugi raz do systemu EZD (Jednokrotne logowanie)
261. EZD musi zapewniać możliwość:
    g. narzucenia minimalnej długości hasła oraz obowiązku wykorzystania różnych rodzajów znaków w haśle (np. liter, cyfr i znaków specjalnych);
    h. ustalenia czasu obowiązywania hasła;

i. automatycznego odrzucania prób ustalenia przez użytkownika trywialnego hasła (np. imienia lub nazwiska użytkownika).

262. EZD musi być wyposażony w filtry umożliwiające wyszukanie odpowiednich dokumentów (i innych obiektów) oraz interesantów według predefiniowanych atrybutów (kryteriów wyszukiwania).
263. System EZD musi pozwalać na odbieranie i wysyłanie dowolnych dokumentów z i do zewnętrznych systemów za pośrednictwem skrytki ePUAP.
264. Środowisko EZD powinno umożliwiać udostępnianie usług WebService.
265. EZD musi zapewniać możliwość integracji z systemem ePUAP, automatyczną rejestrację i wysyłanie dokumentów, weryfikację podpisów i paczek ePUAP oraz wizualizacji dokumentów pobranych z ePUAP oraz UPO, UPD i UPP.
266. EZD musi zapewnić podpisywanie pojedynczych i wielu pism i załączników podpisem elektronicznym kwalifikowanym z poziomu aplikacji, weryfikację podpisu.
267. EZD musi zapewniać możliwość podpisywania pism za pomocą Profilu Zaufanego (PZ).
268. EZD musi zapewniać możliwość podpisywania pism i załączników za pomocą kwalifikowanej pieczęci elektronicznej.
269. EZD musi zapewniać współpracę z urządzeniami wspomagającymi rejestrację dokumentów, a w szczególności: skanerami; czytnikami kodów kreskowych; drukarkami etykiet adresowych i kodów kreskowych
270. EZD musi umożliwiać definiowanie uprawnień każdego ze stanowisk w zakresie: dostępu do odpowiednich modułów, w tym dokumentów i spraw oraz uprawnień do aktualizacji i przeglądania ich zawartości.
271. EZD musi umożliwiać wymuszanie zmiany hasła po upływie czasu, określonego przez Administratora.
272. EZD musi cechować się rozbudowanym modułem bezpieczeństwa zarządzającym dostępem użytkowników do funkcji systemu. Musi zapewnić dostęp do wybranych funkcji administracyjnych dla uprawnionych pracowników.
273. Panel administracyjny EZD musi umożliwiać uprawnionym Użytkownikom, zdefiniowanie i prowadzenie rejestrów wszystkich typów dokumentów z zakresu działalności Zamawiającego zgodnie z wymaganiami prawnymi dotyczącymi tych dokumentów (np. ewidencja decyzji, zaświadczeń itd.).
274. EZD musi zapewnić: odwzorowanie struktury organizacyjnej urzędu (komórek, pracowników, stanowisk) z możliwością modyfikacji, przydzielanie zdefiniowanym grupom użytkowników uprawnień do wykonywania określonych funkcji.
275. Panel administracyjny EZD musi umożliwiać przeglądanie historii logowania użytkowników.
276. EZD musi umożliwiać zarządzanie słownikiem Jednolitego Rzeczowego Wykazu Akt i nadawanie uprawnień dla poszczególnych klas.
277. Panel administracyjny EZD musi umożliwiać zarządzanie kontami, w minimalnym zakresie:
    j. edycji uprawnień,
    k. musi umożliwiać zarządzanie i określanie przez Administratora wymaganej złożoności hasła,
    l. określanie co najmniej: maksymalnej i minimalnej długości hasła, czasu ważności hasła,
    m. ustawienia praw dostępu dla stanowiska.
278. EZD musi zapewniać funkcjonalność zarządzania dostępem do aplikacji:
    n. Administrator systemu musi mieć możliwość tworzenia, modyfikacji oraz dezaktywacji kont użytkowników,
    o. Administrator systemu, użytkownik może nadawać uprawnienia innym użytkownikom,
    p. Administrator systemu może przypisywać użytkowników do grup,
    q. System musi pozwalać na wygenerowanie linka do zmiany hasła dla użytkownika.

Wymagania Funkcjonalne EZD

279. EZD musi obsługiwać rejestrację przesyłek przychodzących, w formie papierowej i elektronicznej (przekazywanych za pośrednictwem Elektronicznej Skrzynki Podawczej na ePUAP, portalu e-usług lub innych skrzynek podawczych oraz poczty elektronicznej).

280. Podczas procesu rejestracji przesyłek przychodzących w formie papierowej, EZD musi umożliwiać skanowanie z wykorzystaniem skanera zgodnego z TWAIN (z poziomu interfejsu aplikacji) poszczególnych dokumentów, wchodzących w skład przesyłki. Interfejs do skanowania musi posiadać, co najmniej narzędzia do edycji obrazu ze skanera poprzez: obrót o dowolny kąt, zmianę kolejności stron, zapis do PNG i PDF, zmiany kontrastu.
281. EZD musi umożliwiać odebranie poczty elektronicznej za pomocą wbudowanego klienta pocztowego POP3 oraz SMTP i umożliwić rejestrację w rejestrze przesyłek wpływających lub bezpośrednie dołączenie wiadomości z załącznikami do akt sprawy.
282. EZD musi umożliwiać opatrywanie przesyłek przychodzących metadanymi zgodnie z instrukcją kancelaryjną.
283. System musi umożliwiać generowanie potwierdzenia przyjęcia przesyłki wpływającej przez punkt kancelaryjny, opatrzonego kodem kreskowym odpowiadającym kodowi kreskowemu przesyłki. Potwierdzenie przyjęcia wygenerowane przez EZD musi umożliwiać zamieszczenie, co najmniej daty wpływu, oznaczenia graficznego jednostki, nazwy jednostki.
284. EZD musi umożliwiać rejestrację zwrotów przesyłek oraz pocztowych potwierdzeń odbioru (zwrotek).
285. EZD musi umożliwiać zarządzanie zakresem zawartości słowników systemowych. Minimalna lista słowników to: JRWA, Gońcy, Rejony, Kody pocztowe, Rodzaje dokumentów, Sposoby dostarczania korespondencji, Sposoby wysyłania korespondencji, Statusy spraw, Sposoby płatności, rodzaje interesantów.
286. EZD musi umożliwiać użytkownikom dekretującym wskazanie jednej lub kilku komórek lub stanowisk merytorycznych odpowiedzialnych za prowadzenie i zakończenie sprawy. W przypadku wyboru kilku osób, możliwe jest wskazanie osoby odpowiedzialnej za ostateczne załatwienie sprawy.
287. EZD musi umożliwiać przekazywanie dokumentów na pojedyncze stanowiska i na wiele stanowisk.
288. System musi pozwalać na wprowadzenie polecenia kierowanego do wszystkich adresatów dekretacji i indywidualnego polecenia dla każdego adresata.
289. EZD musi umożliwiać dekretacje dokumentu ze wskazaniem komórki wiodącej, współpracującej oraz do wiadomości
290. EZD musi umożliwiać tworzenie kopii dokumentu na podstawie oryginału, kopii i do wiadomości.
291. Utworzona kopia powinna mieć właściwości maksymalnie takie jak dokument w oparciu o który powstała (np. z dokumentu do wiadomości nie może powstać kopia).
292. System musi pilnować, by dokument w trakcie kolejnych dekretacji był zadekretowany maksymalnie z ustawieniem takimi, jak został zadekretowany krok wcześniej (np. w przypadku pierwszej dekretacji kopii dokumentu, kolejna dekretacja nie może się odbyć na oryginale na stanowisku, które otrzymało kopię).
293. EZD powinno pozwalać administratorom na zdefiniowanie domyślnej grupy osób do których dekretowany będzie dokument.
294. EZD musi umożliwić odróżnienie oraz jednoznaczną identyfikację i odrębne przetwarzanie poszczególnych dokumentów, przechowywanych w postaci odwzorowań cyfrowych wchodzących w skład przesyłki, przy zachowaniu ich powiązania z przesyłką.
295. EZD musi umożliwić dodawanie przez użytkownika informacji opisujących poszczególne dokumenty, przesyłki lub sprawy w postaci notatek, zgodnie z instrukcją kancelaryjną.
296. EZD musi umożliwiać dwustronną komunikację z systemem ePUAP (odbieranie – wysyłanie dokumentów).
297. EZD musi automatyczne przypisywać UPP i UPD do wysłanych dokumentów przez ESP.
298. EZD musi posiadać wbudowany edytor tworzenia szablonów dokumentów służący do tworzenia dokumentów wewnątrz systemu, bez konieczności używania zewnętrznych aplikacji.
299. EZD musi obsługiwać szablony dokumentów co najmniej w zakresie:
    a. możliwości zdefiniowania szablonu dokumentu oraz przypisania do niego uprawnień dla stanowisk lub komórek organizacyjnych,
    b. możliwość tworzenia szablonów w zależności od typu dokumentu: korespondencja wychodząca, dokument wpływający, dokument wewnętrzny,
    c. prowadzenia repozytorium szablonów, które umożliwia zarządzanie szablonami,

d. możliwości wstawiania znaczników do szablonu. Minimalny zakres znaczników:
e. dane nadawcy,
f. dane adresata (min. imię, nazwisko, adres, nazwa instytucji),
g. kod kreskowy,
h. pełne dane pracownika prowadzącego sprawę,
i. znak pisma/sprawy,
j. adresaci pisma,
k. data pisma,
l. lista stron sprawy,
m. elementy pozwalające na sterowanie zawartością dokumentu np. znacznik nowej strony,
n. możliwości wykorzystania zdefiniowanego szablonu przy tworzeniu pism wychodzących z autouzupełnianiem zawartości w/w znaczników,
o. możliwości generowania korespondencji seryjnej.

300. Każdy dokument opiera się o indywidualny szablon dokumentu, który jest definiowany w systemie.
301. Każdy szablon może posiadać dowolną liczbę kontrolek.
302. W przypadku rejestracji dokumentu XML (zgodnego z CRD) system musi automatycznie kopiować dane z poszczególnych węzłów dokumentu XML do odpowiednich kontrolek.
303. System musi umożliwić eksport dokumentu systemowego do następujących formatów: XML (zgodnego z CRD), PDF, DOCX, ODT.
304. EZD musi umożliwiać integrację z pakietem MS Office, OpenOffice i LibreOffice co najmniej w zakresie możliwości edycji dokumentów wychodzących (pisma, arkusze) dołączanych przez użytkowników do spraw bezpośrednio w pakiecie MS Office, OpenOffice i LibreOffice, EZD musi umożliwiać import tekstu przygotowanego w zewnętrznym procesorze tekstu.
305. EZD musi umożliwić generowanie i drukowanie nalepek z kodami kreskowymi na dokumenty papierowe oraz nośniki i odnajdywanie na podstawie zeskanowanej nalepki odwzorowania cyfrowego bądź metryki danego dokumentu.
306. EZD musi umożliwiać generowanie kopert/naklejek dla korespondencji wychodzącej wraz z kodem kreskowym zawierającym unikatowy identyfikator wysyłki.
307. System musi pozwalać na łączenie wielu przesyłek wychodzących w jedną kopertę, w przypadku, gdy użytkownik stwierdzi, iż dotyczą one tego samego adresata.
308. EZD musi być zintegrowane z programem obsługującym pocztę tradycyjną w zakresie automatycznego przesyłania listy przesyłek oraz odbioru z tejże aplikacji, informacji o numerze nadanym przesyłce, doręczeniu, ZPO lub zwrocie przesyłki. System musi umożliwiać wydruk książki nadawczej oraz dziennika korespondencji.
309. System musi umożliwiać tworzenie własnych cenników przesyłek uwzględniających formę wysyłki, wagę i gabaryt.
310. EZD musi prezentować informacje na temat statusu przeczytania zadekretowanego/przekazanego dokumentu i na tej podstawie umożliwiać cofnięcie wykonanej czynności.
311. EZD musi umożliwić rejestrację historii pisma (czynność wykonana, data i czas, użytkownik) dokumentów papierowych (dla których istnieje odwzorowanie cyfrowe oraz dla których nie zostało ono wykonane) oraz nośników.
312. EZD musi umożliwić wszczynanie, prowadzenie i załatwianie spraw, przechowywanie akt sprawy i prowadzenie spisów spraw zgodnie z obowiązującymi przepisami. System automatycznie musi nadawać znak sprawy i zapewnia jego zgodność z wymogami instrukcji kancelaryjnej.
313. EZD musi umożliwić prowadzenie rejestrów kancelaryjnych, w tym rejestru przesyłek wpływających, wychodzących oraz pism wewnętrznych.
314. EZD musi umożliwić numerację i klasyfikację spraw w oparciu o JRWA zgodnie z instrukcją kancelaryjną.
315. EZD musi umożliwiać określenie terminu realizacji spraw w oparciu o dane JRWA.
316. EZD musi umożliwiać oddzielną rejestrację dokumentów nietworzących akt sprawy, w szczególności:

p. rejestru faktur – wyposażonego w opcję wieloetapowego zatwierdzania faktury i potwierdzania płatności faktury przez uprawnionych użytkowników wraz z mechanizmem wizualnego oznaczania faktur przeterminowanych,

q. definiowania z poziomu administratora systemu dowolnego rejestru poprzez:

r. definicję pól i typów pól dokumentów wchodzących w skład rejestru,

s. możliwość definiowania masek w polach rejestru,

t. definiowanie uprawnień (podglądu, edycji),

u. możliwość udostępnienia zawartości rejestru na BIP.

317. EZD musi umożliwiać wielostopniowy proces akceptacji dokumentów (zgodnie z instrukcją kancelaryjną podmiotu), z możliwością parametryzacji wymagalności akceptacji dla dokumentu przed jego wysłaniem do interesanta. System musi mieć możliwość wymuszenia przez użytkownika dokonania akceptacji dokumentu z podpisem (podpisem zaufanym, podpisem kwalifikowanym, pieczęcią elektroniczną).
318. Użytkownik powinien mieć możliwość swobodnego definiowania ścieżek akceptacji (wskazania konkretnych osób oraz liczby pozytywnych zatwierdzeń dla każdego etapu akceptacji).
319. EZD musi umożliwić zapis projektów pism przekazywanych pomiędzy użytkownikami lub komórkami w trakcie załatwiania sprawy, a także zamieszczanie komentarzy odnoszących się do projektów pism.
320. EZD musi zapewnić prowadzenie, podgląd oraz wydruk metryki sprawy zgodnie z obowiązującymi przepisami.
321. EZD musi umożliwić opisywanie spraw i akt sprawy metadanymi zgodnie z obowiązującymi przepisami.
322. EZD musi umożliwić odnotowanie wysyłki przesyłek wychodzących w rejestrze i opatrzenie ich metadanymi zgodnie z przepisami.
323. EZD musi umożliwiać dostarczanie dokumentów za pośrednictwem gońców.
324. EZD musi umożliwiać obsługę gońców w zakresie umożliwiającym gońcom prowadzenie własnych książek nadawczych wraz z możliwością oznaczania statusów przesyłek w ramach książek z poziomu dedykowanej aplikacji na urządzenie mobilne.
325. Dedykowana aplikacja mobilna dla gońców powinna umożliwiać interesantom złożenie podpisu odręcznego na urządzeniu mobilnym, potwierdzającego odbiór przesyłki. Podpis powinien być oznaczony danymi geolokalizacyjnymi.
326. Dedykowana aplikacja dla gońców powinna w czasie rzeczywistym (na określone zdarzenie w aplikacji) przekazywać informacje o statusie przesyłek wraz z jej wszystkimi cechami (podpis, lokalizacja) z wykorzystaniem dedykowanego API.
327. EZD w ramach obsługi gońców musi umożliwiać rejonizację mieszkańców. Oznacza to, ze administrator systemu musi mieć możliwość utworzenia rejonu i przypisania konkretnego gońca do obsługi danego rejonu.
328. EZD musi zapewnić przydzielanie spraw i korespondencji, przekazanych na dane stanowisko, konkretnym użytkownikom pracującym na tym stanowisku.
329. EZD musi umożliwić podgląd historii sprawy, ścieżki obiegu sprawy w taki sposób by możliwe było odwzorowanie pełnego przebiegu sprawy.
330. EZD musi umożliwiać grupowanie dynamiczne spraw w projekty, określenie członków grupy projektowej oraz praw dostępu do projektu.
331. EZD musi posiadać funkcjonalność obsługi kalendarzy. Każdy z użytkowników powinien posiadać dostęp do własnego kalendarza z możliwością dodawania do niego dowolnych zdarzeń. Użytkownik powinien mieć możliwość określenia typu zdarzenia oraz jego opisu. Użytkownik powinien mieć również możliwość definiowania zdarzeń całodniowych i dłuższych oraz cyklicznych. System ma umożliwiać przeglądanie kalendarzy podwładnych. Kalendarz musi umożliwiać dodawanie i edycję wpisów za pomocą mechanizmu „przeciągnij i upuść”.
332. EZD musi posiadać funkcjonalność planowania i raportowania spotkań, co najmniej w zakresie:

v. opracowywanie agendy spotkania,

w. zapraszanie uczestników,

x. wyszukiwanie spotkań,

y. pisanie raportów ze spotkań na podstawie agendy (również przy jej braku),

z. zakładanie kolejnych spraw na podstawie protokołu za spotkania.

333. EZD musi umożliwiać zarządzanie zasobami poprzez ustalanie rezerwacji zasobów. System musi umożliwić definiowanie dowolnych zasobów. Każdy zasób musi być powiązany ze „swoim" terminarzem, w którym to uprawnieni użytkownicy mają wgląd. Ponadto tylko uprawnieni użytkownicy mogą rezerwować zasoby, a jej fakt jest odnotowywany w terminarzu zasobu. Musi również istnieć możliwość grupowania zasobów (np. grupa „pojazdy" zawierająca pojazdy, którymi dysponuje Urząd).
334. EZD musi posiadać funkcjonalność pozwalającą na zbiorcze podejrzenie dostępności rezerwowanych zasobów i innych użytkowników. Każdy terminarz musi być możliwy do przeglądania w trybie dziennym, tygodniowym, miesięcznym.
335. EZD musi być wyposażony w funkcjonalność komunikatora tekstowego. Komunikator musi być integralnym elementem EZD. Komunikator musi umożliwić prowadzenie rozmów pomiędzy dwoma użytkownikami lub prowadzenie rozmów grupowych.
336. EZD musi umożliwić użytkownikowi podgląd przypisanych do niego spraw i korespondencji, z możliwością sortowania, filtrowania i przeszukiwania.
337. EZD musi mieć umożliwić wprowadzanie zmian kadrowych, urlopów i zastępstw. Umożliwia przekazanie osobie zastępującej części lub całości uprawnień osoby zastępowanej. Uprawnienia muszą być przekazane na określony czas dat lub bezterminowo.
338. EZD musi posiadać moduł urlopów umożliwiający co najmniej:
    aa. obsługę wniosków urlopowych umożliwiający złożenie wniosku przez pracownika oraz późniejszą akceptację przez kierownika oraz ostateczne zatwierdzenie przez kadrową,
    bb. wyznaczanie zastępstw na podstawie udzielonych urlopów,
    cc. integracje funkcjonalności urlopów z kalendarzem systemowym co najmniej w zakresie widoku planowanych urlopów uzależnionego od posiadanych uprawnień tj., pracownik widzi swoje urlopy, kierownik widzi urlopy swoje jak i pracowników podległych, kadrowa widzi urlopy wszystkich pracowników,
    dd. informowanie w momencie dekretacji o nieobecności pracownika, na którego dekretowany jest dokument.
339. EZD musi umożliwiać definiowanie zastępstw na czas nieobecnościci polegających na udzieleniu pełnomocnictwa innemu użytkownikowi do wykonywania czynności w imieniu użytkownika nieobecnego. Pełnomocnictwo powinno być definiowane w określonym przedziale czasu. Dostęp do danych nieobecnego użytkownika powinien być kontrolowany przez System i odbierany wraz z upłynięciem daty końcowej. W trakcie trwania zastępstwa w systemie jest prezentowana informacja o zastępowaniu jednej osoby przez drugą. Wszystkie operacje wykonywane w zastępstwie powinny być zapisane w sposób umożliwiający jednoznaczne określenie, kto wykonał daną operację.
340. EZD musi posiadać moduł obsługi delegacji umożliwiający obsługę wniosków o delegację krajową i zagraniczną oraz późniejszą akceptację przez kierownika.
341. EZD musi umożliwiać przekazywanie spraw na inne stanowisko lub do innej komórki organizacyjnej.
342. EZD musi umożliwić prowadzenie książki teleadresowej interesantów.
343. EZD musi posiadać wewnętrzny edytor, służący do sporządzania komentarzy załączanych do akt sprawy.
344. System musi udostępniać zestaw raportów niezbędnych do pracy urzędu. Użytkownik musi mieć możliwość określenia podstawowych parametrów raportów (okres za jaki raport będzie generowany, sposób sortowania). System musi umożliwiać wygenerowanie co najmniej następujących raportów:
    ee. Statystyki dla spraw;
    ff. Statystyki dla pism:
    gg. Raport pism przychodzących;
    hh. Raport pism przekazanych na stanowisko;
    ii. Raport pism wychodzących;
    jj. Raport z książki doręczeń;
    kk. Raport dekretacji;
    ll. Raport zwrotów;

mm. Raport dokumentów interesanta;
kk. Raport udostępnień danych osobowych;
oo. Koszty wysyłek dokumentu;
pp. Raport terminowości pracowników.

345. Raporty muszą być zwizualizowane w postaci tabeli oraz wykresu.
346. Raporty można wygenerować dla całego urzędu, referatu, biura lub konkretnego pracownika.
347. EZD musi posiadać interfejsy komunikacyjne z Platformą usług informatycznych ePUAP – w zakresie dwukierunkowej integracji z usługą Elektronicznej Skrzynki Podawczej dostępną na ePUAP.
348. EZD ma mieć możliwość importu skrytek podawczych podmiotów z platformy ePUAP.
349. EZD musi posiadać moduł (funkcjonalność) zapewniający obsługę składów chronologicznych dla dokumentów papierowych -archiwum zakładowe umożliwiające: przekazywania dokumentacji przez komórki organizacyjne do archiwum zakładowego, wypożyczania dokumentów, brakowania, wycofywania dokumentacji itd.
350. EZD musi umożliwić dokumentowanie wyjęcia dokumentacji ze składu chronologicznego lub ze składu informatycznych nośników danych oraz wydrukowanie karty zastępczej dla wypożyczanego nośnika. Procedura obsługi składów powinna być realizowana w następujący sposób: pracownik sprawdza dostępność nośnika a następnie składa wniosek o wypożyczenie, osoba obsługująca skład akceptuje wniosek i wypożycza nośnik, zwrot nośnika również jest potwierdzany przez osobę obsługującą skład.
351. EZD musi zapewnić przejmowanie dokumentacji przez archiwum zakładowe po upływie okresu przewidzianego w instrukcji kancelaryjnej. Przejęcie dokumentacji musi polegać na przekazaniu archiwiście uprawnień do tej dokumentacji w systemie EZD oraz ograniczeniu uprawień komórki merytorycznej, zgodnie z instrukcją kancelaryjną.
352. EZD musi posiadać dedykowane funkcje do udostępniania i wycofywania dokumentacji elektronicznej z archiwum zakładowego.
353. EZD musi umożliwiać wypożyczanie spraw z archiwum, podgląd informacji o sprawie oraz zmianę kategorii archiwalnej sprawy przechowywanej w archiwum
354. EZD musi posiadać funkcje wspierające proces porządkowania dokumentacji w archiwum zakładowym (wskazanie dokumentacji wymagającej uzupełnienia).
355. EZD musi realizować brakowanie akt elektronicznych oraz przekazanie akt do archiwum państwowego oraz sporządzenie i przechowywanie odpowiedniej dokumentacji.
356. EZD musi wspierać pracę archiwisty poprzez automatyczne typowanie dokumentacji do brakowania lub przekazania do archiwum państwowego (po upływie terminów związanych z danymi kategoriami archiwalnymi).
357. EZD musi wspomagać użytkownika w przygotowywaniu paczki archiwalnej dla Archiwum Państwowego poprzez przygotowywanie automatycznych spisów zdawczo-odbiorczych, wykazu akt, oraz zapisanie spraw w strukturze wymaganej przez Archiwum Państwowe.
358. EZD musi umożliwiać sporządzenie pocztowej książki nadawczej dostosowanej do zróżnicowanych wymagań występujących w różnych urzędach pocztowych.
359. EZD musi posiadać wbudowany mechanizm powiadomień, informujący o istotnych zdarzeniach związanych z jego aktywnością w systemie. Minimalny zbiór powiadomień powinien obejmować informowanie o: zadekretowaniu dokumentu na pracownika, przekazaniu dokumentu do akceptacji, akceptacji dokumentu, udostępnieniu dokumentu pracownikowi.
360. EZD musi posiadać mechanizm parafowania dokumentów oraz podpisywania ich kwalifikowanym podpisem elektronicznym. W przypadku dokumentów podpisanych – istnieje możliwość weryfikacji złożonego podpisu oraz wydrukowania raportu z podpisu.
361. Klient ESP musi mieć możliwość obsługi wielu skrytek jednocześnie.
362. Klient ESP musi mieć możliwość wyświetlania dowolnego dokumentu XML. Jeśli dokument XML nie posiada wskazania na XSL lub wskazane XSL nie jest dostępne, klient ESP musi rozpoznać taką sytuację i wyświetlić wszystkie węzły tego dokumentu XML.
363. Klient ESP musi prawidłowo wyświetlać każdy dokument zgodny z CRD.

364. Klient ESP musi automatycznie wyłuskiwać następujące dane z dokumentu XML (zgodnego z CRD): załączniki, dane nadawcy i odbiorcy z węzła Dane Dokumentu oraz informacje o osobie, która podpisała dokument podpisem kwalifikowanym lub Profilem Zaufanym.
365. Klient ESP musi umożliwić automatyczne weryfikowanie podpisu złożonego za pomocą Podpisu Zaufanego.

Administracja systemie EZD i warunki techniczne

366. EZD musi umożliwić modelowanie wielopoziomowej struktury organizacyjnej instytucji, która umożliwi przypisanie pracowników do odpowiednich stanowisk a także wprowadzanie modyfikacji w strukturze w ramach zmian organizacyjnych za pomocą dezaktywacji i aktywacji stanowisk i komórek organizacyjnych
367. EZD musi umożliwić definiowanie uprawnień do poszczególnych funkcji systemu oraz grupowanie uprawnień w role w celu ułatwienia administracji systemem.
368. Uprawnienia i role przypisywane są do stanowiska, a nie do użytkownika systemowego.
369. Użytkownik logując się do systemu, ma dostęp do określonych obszarów systemu na podstawie uprawnień, które posiada stanowisko, do którego jest przypisany użytkownik.
370. EZD musi umożliwiać delegowanie części lub całości posiadanych uprawnień.
371. System musi posiadać wyodrębniony moduł administracyjny. Dostęp do tego modułu mogą uzyskać jedynie użytkownicy z odpowiednimi uprawnieniami.
372. EZD musi posiadać rozbudowany rejestr zdarzeń rejestrujący akcje użytkowników na obiektach systemowych, udane i nieudane próby logowania oraz typowe błędy aplikacji.
373. EZD umożliwi zarządzanie uprawnieniami w oparciu o grupy uprawnień i grupy zasobów, jakich dotyczą. System uprawnień musi być zdolny do odzwierciedlenia uprawnień i odpowiedzialności poszczególnych pracowników wynikający z Instrukcji Kancelaryjnych oraz struktury stanowisk.
374. Hasła w EZD muszą być przechowywane w systemie w formie zaszyfrowanej - nie może być możliwości ich odtworzenia, lecz jedynie zresetowania. Po zresetowaniu hasła użytkownika przez administratora system musi wymagać od użytkownika zdefiniowania nowego hasła przy pierwszym logowaniu.
375. EZD musi umożliwiać swobodne definiowanie polityki uwierzytelniania i blokowania kont w oparciu o następujące parametry:
    a) Minimalna długość nazwy użytkownika i hasła
    b) Ilość dużych liter, cyfr, znaków specjalnych w haśle,
    c) Długość cyklu wymuszania zmiany hasła (w miesiącach),
    d) Ilość nieudanych prób logowania, po których następuje blokada konta,
    e) Czas blokady konta po przekroczeniu liczby nieudanych prób logowania.
376. Zakres wartości w słownikach prowadzonych przez system powinien być konfigurowalny przez administratora lub pochodzić z rejestrów centralnych (np. TERYT).
377. System w przypadku rejestrów centralnych powinien umożliwiać wyłączenie walidacji pól które wykorzystują dany rejestr (np. Teryt i pola adresowe) tak by użytkownik mógł dane wprowadzić samodzielnie.
378. EZD musi rejestrować wszystkie czynności dostępu do usług i zasobów w systemie, w tym informacje o:
    a) operacjach na dokumentach,
    b) operacjach na danych osobowych,
    c) zmianach haseł,
    d) zdarzeniach uwierzytelniania (udane logowanie, wylogowanie, nieudane logowanie);
    e) zdarzeniach autoryzacji (nieudane/udane operacje);
    f) zdarzeniach administracyjnych.

379. Zapisywanie danych identyfikujących musi obejmować:
    a) adres IP i nazwę maszyny, z której wykonano daną czynność;
    b) identyfikator/nazwa użytkownika, który wykonał daną czynność;
    c) czas wystąpienia.
380. EZD musi posiadać mechanizm informujący użytkownika o wprowadzonych zmianach w aplikacji.

Rezultaty, które muszą zostać osiągnięte w związku z integracją EZD z Portalem e-Urząd oraz aplikacją mobilną

381. EZD musi wyświetlać dokumenty wysłane z portalu e-usług lub aplikacji mobilnej w sposób sformatowany przez styl, na który dokument wskazuje nawet jeśli CRWDE nie jest dostępne w danej chwili.
382. EZD musi udostępniać dla Portalu e-Urząd możliwość przesyłania informacji zwrotnej dotyczącej danej sprawy w postaci publikacji statusu sprawy automatycznie generowanego w systemie EZD na każdym etapie procesu rozpatrywanej sprawy.
383. EZD musi przekazywać do Portalu e-Urząd informację o symbolu, pod jakim dokument został zarejestrowany w dzienniku korespondencji przychodzącej.
384. EZD musi przekazywać dokument do portalu e-usług, na konto adresata, jeśli dokument z systemu EZD został wysłany bez potwierdzenia.
385. EZD musi przekazywać informacje o oczekującej korespondencji do Portalu e-Urząd, na konto adresata, jeśli dokument z systemu EZD został wysłany z potwierdzeniem odbioru.
386. EZD musi przekazywać dokument do Portalu e-Urząd, na konto adresata, jeśli dokument z systemu EZD został wysłany z potwierdzeniem odbioru i system EZD otrzymał już UPD do tego dokumentu.
387. EZD musi wyświetlić informacje o wniesionej płatności, jeśli była wymagana przy danej e-usłudze wysłanej poprzez Portal e-Urząd lub aplikację mobilną. Sposób prezentowania informacji o płatności musi jednoznacznie identyfikować płatność we wpływach Urzędu.
388. Przesłanie zgody użytkownika na otrzymywanie dokumentów z Portalu e-Urząd lub aplikacji mobilnej w postaci elektronicznej jest przekazywana do EZD. Informacja o wyrażonej zgodzie musi być umieszczona przy danym interesancie w bazie interesantów.
389. Pisma przychodzące z Portalu e-Urząd i aplikacji mobilnej będą rejestrowane i dekretowane w EZD.
390. EZD musi odbierać dokumenty z poszczególnych dedykowanych skrytek ESP przekazywanych z Portalu e-Urząd i aplikacji mobilnej.

Wymagana Specyfikacja Techniczna Oprogramowania do zarządzania siecią i jej bezpieczeństwem

Oprogramowanie powinno posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source, nie powinien być objęty limitem ilości danych, baza danych nie powinna wymagać dodatkowego licencjonowania.

Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Powinny one być również grupowane w osobnym, dedykowanym oknie.

Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, powinien być objęty kontrolą na poziomie wybranych Administratorów – program powinien mieć możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator powinien mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. możliwość wyłączenia zdalnej deinstalacji Agenta, ograniczenie dostępu do Opcji programu oraz logów działań innych administratorów. Program powinien posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta.

Działania administratorów powinny być automatycznie eksportowane do zewnętrznego kolektora Syslog.

MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) powinno obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

1. wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
2. wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
3. wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
4. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
5. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku.
6. wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze.
7. wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie.
8. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny.
9. zablokowania mapy urządzeń przed przypadkową edycją.
10. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów.
11. serwerów pocztowych:
    -program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty,

-program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
-program ma możliwość wykonywania operacji testowych,
-program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.

12. monitorowania serwerów WWW i adresów URL.
13. cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.
14. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
15. obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np.
16. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID.
17. obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.
18. monitoringu routerów i przełączników wg:
    -zmian stanu interfejsów sieciowych,
    -ruchu sieciowego,
    -podłączonych stacji roboczych – graficzna prezentacja panelu switcha, - ruchu generowanego przez podłączone do portów stacje robocze.
19. serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie.
20. wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu.
21. wydajności systemów Windows:
    - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Program powinien posiadać Inteligentne Mapy i Oddziały oraz funkcję kompilatora plików MIB, który umożliwi dodawanie definicji dla modułów SNMP.

Program powinien umożliwiać definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy powinny być budowane przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.

Program powinien mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

W **ZAKRESIE INWENTARYZACJI** program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.

2. Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.

3. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwi audytowanie i weryfikację użytkowania licencji w organizacji.

4. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.

5. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.

6. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).

7. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.

8. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.

9. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).

10. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji powinny być logowane.

Moduł inwentaryzacji zasobów powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
2. tworzenia powiązań między zasobami a urządzeniami,
3. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
4. wskazania osób uprawnionych do użycia zasobów,
5. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
6. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
7. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
8. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
9. importu danych z zewnętrznego źródła (.CSV),
10. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
11. tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
12. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
13. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
14. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
15. generowania protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
16. archiwizacji i porównywania audytów zasobów,
17. tworzenia kodów kreskowych dla zasobów,
18. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
19. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej na system Android,
20. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
21. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Dodatkowo dostępny powinien być Agent inwentaryzacji na system Android.

Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.

2. Informacje o aplikacjach używanych w organizacji.

3. Tworzenie własnych wzorców aplikacji.

4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.

5. Informacje o komputerach, na których aplikacja została wykryta.

6. Zarządzanie posiadanymi licencjami.

7. Wskazywanie osób odpowiedzialnych za licencję.

8. Wskazanie użytkowników licencji.

9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.

10. Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.

12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.

13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe powinny posiadać możliwość filtrowania elementów per oddział.

W **ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW** program powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

1) Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),

2) Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,

3) Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,

4) Informacji o edytowanych przez użytkownika dokumentach,

5) Historii pracy (cykliczne zrzuty ekranowe),

6) Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),

7) Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),

8) Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma

możliwość monitorowania kosztów wydruków, nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program powinien również posiadać możliwość:

1) blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen powinny być tworzone dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

2) blokowania ruchu na wskazanych portach TCP/IP,

3) blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,

4) wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,

5) przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),

6) definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Program powinien posiadać możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

Program powinien posiadać mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji powinny być tworzone dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

Program powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

PROGRAM POWINIEN UMOŻLIWIAĆ REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika dostępny powinien być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). W module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które zostaną przetworzone i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Moduł powinien umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Użytkownicy powinni posiadać możliwość monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł powinien również zawierać komunikator (czat), który umożliwiać będzie przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadania artykułom statusów. Program powinien umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy.

Moduł powinien umożliwiać uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

Moduł pomocy zdalnej powinien umożliwiać również:

1) pobieranie listy użytkowników z Active Directory,

2) zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,

3) zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,

4) zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,

5) tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,

6) automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,

7) procesowanie zgłoszeń użytkowników z wiadomości e-mail,

8) tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,

9) wykonywanie operacji na wielu zgłoszeniach równocześnie,

10) dołączanie załączników do zgłoszeń,

11) rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,

12) szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,

13) wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,

14) zrzuty ekranowe (podgląd pulpitu),

15) dystrybucję oprogramowania przez Agenty,

16) dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),

17) zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,

18) możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,

19) planowanie nieobecności pracowników helpdesk,

20) obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,

21) generowanie raportów obsługi helpdesk,

22) zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),

23) zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),

24) wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

Oprogramowanie powinno umożliwiać **OCHRONĘ DANYCH PRZED WYCIEKIEM** poprzez blokowanie urządzeń:

1. Blokowanie urządzeń i nośników danych.

Program powinien umożliwiać zarządzanie prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.

3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.

5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.

6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.

7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.

8. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - blokowanie prywatnych urządzeń.

3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.

4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.

5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

2. Podłączenie/odłączenie urządzenia przenośnego.

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

Program powinien dostarczać informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji powinien mieć możliwość oznaczenia sesji aktywności jako czas prywatny, gdy wykonuje czynności prywatne na sprzęcie firmowym. Menedżerowie oraz przełożeni powinni mieć automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz możliwość przeanalizowania aktywności w danym okresie. Pracownik

powinien mieć możliwość przeglądania swoich historycznych danych, wybierając okres aktywności, który go interesuje.

1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.

2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.

3. Statystyki aktywności podwładnych widoczne dla przełożonego.

4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.

5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.

6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.

7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.

8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.

9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.

10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).

11. Wskaźnik czasu poświęconego na aktywność produktywną.

12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.

13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.

14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji.

Portal informacyjny w formie platformy WWW

Oprogramowanie powinno posiadać obszar funkcjonalny w formie platformy WWW, który pozwalać będzie na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety powinny być rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych powinna być automatycznie odświeżana oraz:

1) Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.

2) Wyświetlana w trybie jasnym lub nocnym.

Oprogramowanie powinno umożliwiać zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.

Widgety powinny prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania:

3) Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,

4) Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,

5) Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW,

6) Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,

7) Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem),

8) Produktywność dla grupy, Statystyki czasu nieproduktywnego.

Ochrona przed usunięciem

Program powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

Funkcjonalność Agenta

Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.