

Opis Przedmiotu Zamówienia

w postępowaniu pn.: „Zakup sprzętu komputerowego i oprogramowania w ramach projektu grantowego "Cyfrowa Gmina"”

Zestawienie sprzętu komputerowego i oprogramowania

Lp.	Nazwa	Ilość
CZĘŚĆ I – sprzęt serwerowy i oprogramowanie		
1.	Serwer z serwerowym systemem operacyjnym – typ A	1
2.	Serwer z serwerowym systemem operacyjnym – typ B	1
3.	Serwer z serwerowym systemem operacyjnym – typ C	1
4.	Serwer (NAS) z dyskami i oprogramowaniem do backupu – komplet	1
CZĘŚĆ II – sprzęt komputerowy		
5.	Stacja robocza – jednostka centralna z monitorem	19
6.	Komputer przenośny	5
7.	Urządzenie wielofunkcyjne	5
8.	Dysk zewnętrzny USB	1
CZĘŚĆ III – oprogramowanie		
9.	Oprogramowanie biurowe	18
10.	Oprogramowanie antywirusowe	150
11.	Specjalistyczne oprogramowanie do blokowania treści niebezpiecznych	135
CZĘŚĆ IV – oprogramowanie specjalistyczne		
12.	Specjalistyczne oprogramowanie do monitorowania stanowiska pracy, kompleksowe zarządzanie infrastrukturą IT, monitorowanie urządzeń sieciowych oraz ochrona przed utratą poufnych danych – komplet	1
13.	Oprogramowanie do zarządzania backupem danych w systemach firmy REKORD	1

Wymagania ogólne

Dostarczony sprzęt musi być fabrycznie nowy, nieużywany (nie dopuszcza się sprzętów odnawianych, demonstracyjnych lub powystawowych), nieuszkodzony, nieobciążony prawami osób trzecich, pierwszej jakości, dostarczony w fabrycznych, oryginalnych opakowaniach identyfikujących sprzęt znajdujący się wewnątrz opakowania.

Dostarczony sprzęt musi pochodzić z oficjalnego kanału sprzedaży producenta na terenie Polski lub Unii Europejskiej.

Gwarancja i serwis sprzętu muszą być realizowane przez producenta lub firmę autoryzowaną przez producenta, lub jego przedstawicielstwo w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji.

Systemy operacyjne oraz pakiety biurowe oprogramowania muszą być fabrycznie nowe, nieużywane, nieaktywowane nigdy wcześniej oraz dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności, na przykład z tzw. naklejkami GML (Genuine Microsoft Label) lub naklejkami COA (Certificate of Authenticity) stosowanymi przez producenta sprzętu lub inną formą uwiarygodnienia

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

oryginalności wymaganej przez producenta oprogramowania stosowną w zależności od dostarczanej wersji.

Dostarczone licencje nie mogą powodować konieczności podpisania przez Zamawiającego dodatkowych umów lub dokumentów.

W ramach procedury odbioru Zamawiający zastrzega sobie prawo weryfikacji czy zaoferowane oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem. W powyższym celu Zamawiający może zwrócić się do przedstawicieli producenta danego oprogramowania z prośbą o weryfikację czy oferowane oprogramowanie i materiały do niego dołączone są oryginalne. W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiety producenta, Zamawiający zastrzega sobie prawo do wstrzymania płatności do czasu dostarczenia oprogramowania i certyfikatów/etykiety należycie licencjonowanych i oryginalnych oraz do odstąpienia od umowy. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań.

Zamawiający jest jednostką administracji publicznej (Jednostką Samorządu Terytorialnego), w związku z czym uprawniony jest do nabywania licencji typu GOVERNMENT.

Użytkownikami końcowymi sprzętu i oprogramowania będą urząd JST (Jednostki Samorządu Terytorialnego – Gminy Zebrzydowice) i jednostki podległe oraz nadzorowane.

Dane użytkownika końcowego zostały podane w celu weryfikacji ew. dodatkowych uprawnień (np. dla jednostek oświatowych), właściwej kalkulacji cenowej, określenia licencjobiorcy oprogramowania itp. oraz wskazania docelowego miejsca używania sprzętu i oprogramowania. Gdy w opisie nie wskazano użytkownika końcowego oznacza to, że będzie nim URZĄD GMINY ZEBRZYDOWICE (Zebrzydowice, ul. ks. Antoniego Janusza 6, 43-410 Zebrzydowice).

I. CZĘŚĆ I – SPRZĘT SERWEROWY I OPROGRAMOWANIE

1. Serwer z serwerowym systemem operacyjnym – typ A – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji minimum 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiającym montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów Intel 3rd Gen. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych.
Procesor	Zainstalowane dwa procesory 8-rdzeniowe, klasy x86, dedykowane do pracy z zaferowanym serwerem, taktowane zegarem minimum 2.8 GHz (częstotliwość bazowa) umożliwiające osiągnięcie wyniku minimum 34 900 punktów w teście PassMark dla konfiguracji Dual CPU- CPU Mark dostępnym na stronie internetowej: https://www.cpubenchmark.net/multi_cpu.html (wyniki z dnia 27.02.2023 załączone do dokumentów postępowania).
RAM	Minimum 32 GB DDR4 RDIMM 3200MT/s w kościach 16GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	Minimum dwa sloty PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Dodatkowa karta sieciowa 4x RJ-45, 1Gb/s, 1000Base-T, PCIe. Wolny wbudowany port w standardzie OCP 3.0. (wolny wbudowany port nie może zmniejszać ilość wbudowanych portów PCIe).
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD. Zainstalowane 2 dyski HDD SAS ISE o pojemności minimum 1.2TB, 12Gb/s, 10 tys. obr./min, Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności minimum 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności minimum 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający minimum 8 GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	Przednie: minimum 1x VGA, minimum 1x USB 2.0, minimum 1x micro-USB dedykowane dla karty zarządzającej, Tyłne: minimum 1x VGA, minimum 2x USB w tym 1x USB 3.0,

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Video	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości minimum 1920x1200
Zasilacze	Redundantne, Hot-Plug minimum 600W każdy.
Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0.
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: 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 autentykację 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.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019, Microsoft Windows Server 2022.
Warunki gwarancji	3 lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 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 autoryzację producenta urządzenia – dokumenty potwierdzające należy załączyć do oferty.

	<p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
Serwerowy system operacyjny	<p>2 x Microsoft Windows Server Standard 2022 64bit dla 16 rdzeni (możliwość uruchomienia 4 wirtualnych środowisk systemu operacyjnego) lub równoważny (kryteria równoważności podano na końcu dokumentu OPZ)</p> <p>1 x Microsoft Windows Server 2022 External Connector lub równoważny (kryteria równoważności podano na końcu dokumentu OPZ)</p> <p>Licencje z możliwością ich przenoszenia na inne urządzenie, z prawem do korzystania z wcześniejszych wersji oprogramowania (downgrade), nie są dopuszczalne licencje trwale przypisane do oferowanego serwera.</p>

2. Serwer z serwerowym systemem operacyjnym – typ B – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiającym montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	Zainstalowany jeden procesor sześciordzeniowy dedykowany do pracy z zaferowanym serwerem, taktowany zegarem min 2.9 GHz (częstotliwość bazowa) umożliwiający osiągnięcie wyniku minimum 16 600 punktów w teście PassMark - CPU Mark dostępnym na stronie internetowej https://www.cpubenchmark.net/high_end_cpus.html (wyniki z dnia 27.02.2023 załączone do dokumentów postępowania).
Pamięć RAM	16 GB pamięci RAM ECC UDIMM w kościach 16 GB o częstotliwości pracy 3200MT/s. Płyta powinna obsługiwać do minimum 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość minimum 1920x1200
Wbudowane porty	minimum 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, minimum 1 port RS232
Gniazda PCI	Minimum 2 sloty PCIe generacji 4

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Interfejsy sieciowe/FC/SAS	Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Kontroler dysków	Sprzętowy kontroler dyskowy, posiadający minimum 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfujących.
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD, NL SAS Zainstalowane 2 dyski HDD SAS ISE o pojemności minimum 1.2TB, 12Gb/s, 10 tys. obr./min, Hot-Plug Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności minimum 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności minimum 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Wentylatory	Minimum 4 wentylatory
Zasilacze	Redundantne, o mocy Maksymalnie 600W.
Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
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.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i

	posiadać status „Certified for Windows” dla systemów Microsoft, Windows Server 2019, Windows Server 2022.
Warunki gwarancji	<p>3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>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 twardey pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzenia – dokumenty potwierdzające należy załączyć do oferty.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera</p>
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Serwerowy system operacyjny	Windows Server Essentials 2022 64bit lub równoważny (kryteria równoważności podano na końcu dokumentu OPZ), fabrycznie zainstalowany przez producenta serwera.

3. Serwer z serwerowym systemem operacyjnym – typ C – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa typu Tower z możliwością instalacji do 8 dysków twardech 3,5”.
Płyta główna	Z możliwością instalacji jednego fizycznego procesora, posiadająca minimum 4 sloty na pamięć RAM UDIMM z możliwością zainstalowania do minimum 128GB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Zainstalowany jeden procesor sześciordzeniowy dedykowany do pracy z zaferowanym serwerem, taktowany zegarem min 2.9 GHz (częstotliwość bazowa) umożliwiający osiągnięcie wyniku minimum 16 600 punktów w teście PassMark - CPU Mark dostępnym na stronie internetowej https://www.cpubenchmark.net/high_end_cpus.html (wyniki z dnia 27.02.2023 załączone do dokumentów postępowania).
Pamięć RAM	16 GB pamięci RAM UDIMM w kościach 16GB o częstotliwości pracy 3200MT/s.
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum 4 sloty PCI Express w tym przynajmniej 2 sloty Gen4

Interfejsy sieciowe/FC/SAS	Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Możliwość instalacji dysków twardych 3,5" typu: SATA, NearLine SAS, SAS, SSD. Zainstalowane 2 dyski SSD SATA o pojemności minimum 480GB, 6Gb/s, Hot-Plug o parametrze DWPD wynoszącym minimum 1. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności minimum 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności minimum 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10.
Wbudowane porty	Minimum 8 portów USB z czego minimum 1 w technologii 3.0 1x RS-232 1x VGA
Video	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Chłodzenie i zasilanie	Wentylator, redundantne zasilacze o mocy minimum 600W wraz z kablami zasilającymi.
Diagnostyka i Bezpieczeństwo	<ul style="list-style-type: none"> • zintegrowany z płytą główną moduł TPM 2.0 • fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: <ul style="list-style-type: none"> • 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 autentykację 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.

Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.</p> <p>Serwer musi posiadać deklaracja CE.</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.</p>
Warunki gwarancji	<p>3 lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzenia – dokumenty potwierdzające należy załączyć do oferty.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
Serwerowy system operacyjny	<p>Windows Server Essentials 2022 64bit lub równoważny (kryteria równoważności podano na końcu dokumentu OPZ), fabrycznie zainstalowany przez producenta serwera.</p>

Użytkownik końcowy:	Ilość
GMINNY OŚRODEK POMOCY SPOŁECZNEJ W ZEBRZYDOWICACH Zebrzydowice, ul. ks. Antoniego Janusza 6, 43-410 Zebrzydowice	1

4. Serwer NAS z dyskami i oprogramowaniem do backupu – 1 komplet

Kompleksowe, zintegrowane rozwiązanie do backupu wraz z usługą wdrożenia zdalnego oraz pomocą techniczną Wykonawcy na okres 1 roku.

W zastosowanym rozwiązaniu oprogramowanie do centralnego zarządzania backupem ma być zintegrowane z platformą sprzętową serwera NAS tak aby nie było potrzeby instalacji serwera backupu (serwera zarządzania) na osobnym serwerze Zamawiającego.

System powinien umożliwić archiwizację 50 stacji roboczych i 5 serwerów oraz 4 hostów wirtualizacji.

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Zamawiający wymaga dostarczenia rozwiązania składającego się z urządzenia NAS, dysków twardej oraz oprogramowania do backupu spełniających poniższe wymagania.

Serwer NAS – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Procesor	Jeden 4-rdzeniowy/8-wątkowy Intel Xeon D-1521 lub równoważny procesor osiągający wynik minimum 5800 punktów w teście PassMark - CPU Mark dostępnym na stronie internetowej https://www.cpubenchmark.net/mid_range_cpus.html (wyniki z dnia 27.02.2023 załączone do dokumentów postępowania). W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net/mid_range_cpus.html , a do oferty należy dołączyć wydruk z tej strony potwierdzający spełnienie wymogu.
Obudowa	Rack o wymiarach maksimum 89 mm x 483 mm x 725 mm; w zestawie szyny teleskopowe do montażu NAS w szafie RACK
Pamięć RAM	8GB DDR4 ECC UDIMM RAM z możliwością rozszerzenia do 64GB
Ilość obsługiwanych dysków	Minimum 12 dysków 3,5"
Interfejsy sieciowe	4 x Gigabit (10/100/1000), Możliwość podłączenia dodatkowej karty 10 Gigabit. Wsparcie dla Link Aggregation, Jumbo Frame oraz WOL.
Porty	2 x USB3.2 Gen 1 2 x Infiniband
Gniazda PCIe	2 x Gen3 x8 slots (x8 link)
Wskaźniki LED	Status, LAN, HDD1 -12
Obsługa RAID	Basic, JBOD, RAID F1,0,1,5,6,10 + Hot Spare 1,5,6,10 i SHR.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych, kluczem AES-256bitów
System Operacyjny	Windows 7 i 10 , MAC OSX 10.11 i nowsze
Licencja na Kamery IP	W zestawie licencja na dwie kamery z możliwością rozszerzenia do 75. Funkcja CMS.
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, WebDAV, CalDAV, SFTP,
Usługi	Wsparcie dla High Availability Serwer VPN Serwer pocztowy dla kilku domen Stacja monitoringu Windows ACL Integracja z Windows ADS Firewall z kontrolą ruchu Serwer WWW

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

	Serwer plików Manager plików przez WWW Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie Antywirus Klient VPN Usługa DDNS Oprogramowanie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware
Klaster HA	Możliwość połączeniu dwóch identycznych urządzeń w jeden klaster wysokiej dostępności (high-availability)
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,
Język GUI	Polski
Gwarancja i serwis	3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta
Waga	Maksimum 15 KG
Certyfikaty	FCC Class A, CE Class A, BSMI Class A
System plików	Dyski wewnętrzne Btrfs, EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT4, EXT3, HFS+, exFAT
Liczba wolumenów	Do 128
Liczba iSCSI Targetów	Do 256
Liczba iSCSI LUN	Do 512
Liczba kont użytkowników	16000
Liczba grup	512
Liczba udziałów	512
Ilość jednoczesnych połączeń	2000 dla CIFS, FTP, AFP – 10000 po rozszerzeniu RAM
Zasilanie	minimum jeden zasilacz wewnętrzny o mocy maksimum 550W
Chłodzenie	FAN x 4 80 x 80 mm

Dyski serwera NAS – 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ dysku	HDD
Format szerokości	3,5"
Pojemność dysku	10 TB
Interfejs dysku	SATA
Prędkość obrotowa dysku	Minimum 7200 obr./min.
Bufor	Minimum 256 KB
Transfer zewnętrzny	Minimum 600 MB/s

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Szybkość transmisji urządzenia	Minimum 600 MBps (zewnętrzna)
Szybkość wewnętrzna danych	Minimum 273 MBps
Niezawodność MTBF	Minimum 2 miliony godziny
Typ pracy	24x7
Błędy nienaprawialne	Maksimum 1 na 10 ¹⁵
Zasilanie Zużycie energii	Maksimum 9.2 W (odczyt) 8.0 W (bezczynność)
Gwarancja	Minimum 5 lat gwarancji door-to-door producenta lub autoryzowanego partnera producenta. W przypadku wystąpienia awarii dysku twardego, uszkodzony dysk twardy pozostaje u Zamawiającego.

Lista funkcji, które muszą być realizowane przez system:

1.	Możliwość backupu stacji roboczych, serwerów, maszyn wirtualnych.
2.	Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich.
3.	Program serwerowy kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10, Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019 Linux, BSD, Mac OS X.
4.	Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10, Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology.
5.	Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików).
6.	Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS).
7.	Automatyczny backup przy wyłączeniu komputera (tylko Windows).
8.	Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?.
9.	Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows).
10.	Backup baz danych i plików poczty w trybie online i offline.
11.	Kopie rotacyjne (wersjonowanie).
12.	Zapis archiwów w otwartym formacie (ZIP 64-bit).
13.	Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi .
14.	Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore).
15.	Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej.
16.	Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych.
17.	Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO.
18.	Możliwość określenia liczby archiwów przechowywanych w miejscu replikacji (mniej lub więcej niż miejscu źródłowym).
19.	Kompresja po stronie stacji roboczej.

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

20.	Replikacja archiwów (automatyczna lub według harmonogramu) na dodatkowy dysk twardy, NAS, serwer FTP.
21.	Centralne sterowanie całym Systemem z jednego miejsca.
22.	Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników.
23.	Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN.
24.	Wysyłanie Alertów administracyjnych na e-mail.
25.	Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych.
26.	Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki.
27.	Automatyczna aktualizacja oprogramowania na komputerach zdalnych.
28.	Bezterminowa licencja - licencja nie może być ograniczona czasowo.
29.	Interfejs, instrukcja i pomoc techniczna w języku polskim.
30.	Rozmiar instalacji klienta < 1MB.

Usługa wdrożenia

Usługa wdrożenia powinna zostać zrealizowana zdalnie, a w jej zakresie powinny zawierać się przynajmniej:

1.	Wysyłka przygotowanej do wdrożenia macierzy NAS (przeprowadzona integracja z oprogramowaniem do backupu),
2.	Konfiguracja serwera backupu,
3.	Przygotowanie paczki instalacyjnej aplikacji klienta backupu,
4.	Omówienie i konfiguracja zadań backupu dla najważniejszych stacji klienckich oraz 3 hostów,
5.	Instruktażowe szkolenie administratora z wdrożonego systemu obejmujące przynajmniej omówienie konfiguracji i funkcji konsoli administracyjnej, procesu odzyskiwania danych oraz najlepszych praktyk dla rozwiązań backupowych.

II. CZĘŚĆ II – SPRZĘT KOMPUTEROWY

5. Stacja robocza – jednostka centralna z monitorem – 19 szt.

Jednostka centralna:

Parametr	Charakterystyka (wymagania minimalne)
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej
Procesor	Minimum 6-rdzeniowy, min 2.50 GHz, osiągający w zaoferowanej konfiguracji wynik minimum 19 000 punktów w teście PassMark - CPU Mark dostępnym na stronie internetowej https://www.cpubenchmark.net (wyniki z dnia 27.02.2023 załączone do dokumentów postępowania). Do oferty należy dołączyć wydruk ze strony http://www.cpubenchmark.net potwierdzający spełnienie wymogu.
Pamięć operacyjna	1 x 16GB 3200 MHz możliwość rozbudowy do min 64GB, minimum 1 slot wolny na dalszą rozbudowę
Parametry pamięci masowej	Minimum 512 GB M.2 SSD NVMe, z możliwością instalacji dodatkowego dysku 2,5" lub 3.5"
Grafika	Zintegrowana w procesorze
Wyposażenie multimedialne	Karta dźwiękowa stereo zintegrowana z płytą główną
Obudowa	Obudowa fabrycznie konwertowalna typu SFF z możliwością pracy w pozycji pionowej i poziomej, min 1 wewnętrzną półkę 3,5"/2,5" dla dysków twardych. Zaprojektowana i wykonana przez producenta komputera opatrzona trwałym logo producenta, metalowa. Obudowa musi dawać możliwość instalacji 1 szt. dysku 3,5" lub 2,5. Zasilacz o mocy maksimum 180W
BIOS	BIOS zgodny ze specyfikacją UEFI
Certyfikaty i standardy	Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)
Warunki gwarancji	2 letnia gwarancja producenta realizowana w miejscu instalacji lub w systemie door-to-door W przypadku wystąpienia awarii dysku twardego, uszkodzony dysk twardy pozostaje u Zamawiającego.
Wsparcie techniczne producenta	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera (ogólnopolski numer) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia: weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć); czasu obowiązywania i typ udzielonej gwarancji.

Wymagania dodatkowe	<p>Zainstalowany system operacyjny Windows 11 Pro 64bit PL lub równoważny (kryteria równoważności podano na końcu dokumentu OPZ).</p> <p>Wbudowane porty i złącza:</p> <ul style="list-style-type: none"> - porty wideo: 1 szt. HDMI, 1 szt. VGA - minimum 8 szt. USB w tym: <ul style="list-style-type: none"> z przodu: 4 porty USB 3.2 Gen 1 Typ-A z tyłu: 3 porty USB 2.0 Typ-A - port sieciowy RJ-45, - porty audio: wyjście słuchawek i wejście mikrofonowe z przodu obudowy; z tyłu port audio Line-out oraz Line-in - 1 półka dla dysku twardego 3,5" zamiennie z możliwością instalacji 1szt dysku 2,5" <p>Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.</p> <p>Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana).</p> <p>Płyta główna wyposażona w:</p> <ul style="list-style-type: none"> - 2 złącza DIMM z obsługą do 64GB pamięci RAM 3200MHz - sloty: 1 szt. PCIe x16, 1 szt. PCIe x1 - 1x złącze M.2 PCIe x1 dla modułu WiFi - 1x złącze M.2 PCIe x1 dla dysku <p>Klawiatura USB w układzie polski programisty</p> <p>Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll)</p> <p>Zainstalowany napęd DVD+/-RW</p>
----------------------------	--

Monitor:

Parametr	Charakterystyka (wymagania minimalne)
Wymiary matrycy	Minimum 23.8"(60.5cm) 16:9 Panoramiczny ekran
Typ matrycy	VA LCD
Rozmiar plamki	Maksimum 0.3 mm
Jasność	250 cd/m2
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy	Maksimum 4ms
Rozdzielczość	Minimum 1920 x 1080
Częstotliwość odświeżania poziomego	30 – 85 kHz
Częstotliwość sygnału analogowego	48 – 75 Hz
Zużycie energii	Maksimum 22W, tryb wyłączenia aktywności mniej niż 0.4W
Podświetlenie	System podświetlenia LED
Bezpieczeństwo	Monitor musi być wyposażony w tzw. Kensington Lock – gniazdo zabezpieczenia przed kradzieżą
Waga bez podstawy	Maksimum 2,65 kg

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Zakres regulacji Tilt	Wymagany, od -5 do +20
Złącze	1 x VGA 1 x HDMI 1 x Audio
Gwarancja	24 miesiące
Inne	Zdejmowana podstawa oraz otwory montażowe VESA

Użytkownik końcowy:	Ilość
URZĄD GMINY ZEBRZYDOWICE Zebrzydowice, ul. ks. Antoniego Janusza 6, 43-410 Zebrzydowice	12
SZKOŁA PODSTAWOWA IM. JAROSŁAWA DĄBROWSKIEGO W KOŃCZYCACH MAŁYCH Kończyce Małe, ul. Jagiellońska 56, 43-410 Zebrzydowice	2
SZKOŁA PODSTAWOWA W MARKŁOWICACH GÓRNYCH Markłowice Górne, ul. Szkolna 25, 43-410 Zebrzydowice	2
SZKOŁA PODSTAWOWA IM. K.K.BACZYŃSKIEGO W ZEBRZYDOWICACH Zebrzydowice, ul. Jana Kochanowskiego 55, 43-410 Zebrzydowice	2
GMINNE PRZEDSZKOLE PUBLICZNE W ZEBRZYDOWICACH Zebrzydowice, ul. Makowa 1, 43-410 Zebrzydowice	1

6. Komputer przenośny – 5 szt.

Parametr	Charakterystyka (wymagania minimalne)
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej,
Matryca	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości FHD (1920 x 1080) z podświetleniem LED matryca matowa, jasność minimum 220nits, kontrast 400:1
Wydajność	Procesor wielordzeniowy osiągający wynik minimum 9 900 punktów w teście PassMark - CPU Mark dostępnym na stronie internetowej https://www.cpubenchmark.net (wyniki z dnia 27.02.2023 załączone do dokumentów postępowania). Do oferty należy dołączyć wydruk ze strony http://www.cpubenchmark.net potwierdzający spełnienie wymogu.
Pamięć RAM	8GB DDR4 możliwość rozbudowy do min 16GB (nie dopuszcza się pamięci wlutowanych); możliwość rozbudowy pamięci przez użytkownika.
Pamięć masowa	minimum 512 GB SSD NVMe, fabryczna możliwość instalacji drugiego dysku 2,5"
Karta graficzna	Zintegrowana z procesorem
Multimedia	Dwukanałowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy minimum 2x 2W, cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa o rozdzielczości minimum HD trwale zainstalowana w obudowie matrycy, dioda informująca użytkownika o aktywnej kamerze.

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Bateria i zasilanie	<p>Czas pracy na baterii minimum 360 minut potwierdzony przeprowadzonym testem MobileMark 25 Battery Life (do oferty załączyć wydruk przeprowadzonego testu)</p> <p>Zasilacz o mocy minimum 65W.</p> <p>Konstrukcja komputera musi umożliwiać demontaż samej baterii lub wszystkich zainstalowanych baterii, samodzielnie bez udziału serwisu w okresie gwarancyjnym. Bateria nie może być trwale zespolona z płytą główną.</p>
Waga	Waga komputera z oferowaną baterią nie większa niż 1,8 kg
Obudowa	Obudowa notebooka wzmocniona, szkielec i zawiasy notebooka wykonany z wzmocnianego metalu.
BIOS	<p>BIOS zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy.</p> <p>BIOS musi umożliwiać przeprowadzenia inwentaryzacji sprzętowej poprzez wyświetlenie informacji o: wersji BIOS, numerze seryjnym i dacie produkcji komputera, wielkości, prędkości i sposobie obsadzenia zainstalowanej pamięci RAM, typie zainstalowanego procesora, zainstalowanym dysku twardym (pojemność, model), MAC adresie wbudowanej w płytę główną karty sieciowej.</p> <p>Funkcja blokowania/odblokowania portów USB</p> <p>Możliwość, ustawienia hasła dla administratora oraz użytkownika dla BIOS'u, po podaniu hasła użytkownika możliwość jedynie odczytania informacji, brak możliwości wł./wył. funkcji. Hasła silne opatrzone o litery, cyfry i znaki specjalne.</p> <p>Możliwość przypisania w BIOS numeru nadawanego przez Administratora.</p>
Bezpieczeństwo	<p>System diagnostyczny z graficzny interfejsem dostępny z poziomu BIOS lub menu BOOT'owania umożliwiający użytkownikowi przeprowadzenie wstępnej diagnostyki awarii poprzez przetestowanie: procesora, pamięci RAM, dysku, płyty głównej i wyświetlacza. Pełna funkcjonalność systemu diagnostycznego musi być dostępna również w przypadku braku lub uszkodzenia oraz sformatowania dysku twardego, braku dostępu do sieci LAN i internetu oraz nie może być realizowana przez narzędzia zewnętrzne podłączane do komputera (np. pamięć USB flash].</p> <p>Dedykowany układ szyfrujący TPM 2.0</p> <p>Złącze na linkę zabezpieczającą przed kradzieżą.</p>
Certyfikaty	<p>Certyfikat ISO 9001 dla producenta sprzętu (załączyć do oferty)</p> <p>Certyfikat ISO 50001 dla producenta sprzętu (załączyć do oferty)</p> <p>Deklaracja zgodności CE (załączyć do oferty)</p> <p>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.</p>
System operacyjny	Zainstalowany system operacyjny Microsoft Windows 11 Professional lub równoważny (kryteria równoważności podano na końcu dokumentu OPZ)
Wymagania dodatkowe	Wbudowane porty i złącza: HDMI 1.4, RJ-45 (karta sieciowa wbudowana), minimum 3xUSB w tym minimum 2 port USB 3.2 gen1 typ-A, czytnik kart SD 3.0, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, złącze zasilania (zasilacz nie może zajmować portów USB)

	Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11AC, moduł bluetooth 4.1 Klawiatura (układ US - QWERTY) z wydzieloną klawiaturą numeryczną, touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów z wbudowanym podświetleniem
Warunki gwarancji	Minimum 2-letnia gwarancja producenta świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego. Dedykowany portal producenta do zgłaszania awarii lub usterek, możliwość samodzielnego zamawiania zamiennych komponentów oraz sprawdzenie okresu gwarancji, fabrycznej konfiguracji. Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. W przypadku wystąpienia awarii dysku twardego, uszkodzony dysk twardy pozostaje u Zamawiającego.

Użytkownik końcowy:	Ilość
SZKOŁA PODSTAWOWA W KACZYCACH Kaczyce, ul. Harcerska 13, 43-417 Kaczyce	3
SZKOŁA PODSTAWOWA IM. K.K.BACZYŃSKIEGO W ZEBRZYDOWICACH Zebrzydowice, ul. Jana Kochanowskiego 55, 43-410 Zebrzydowice	1
GMINNE PRZEDSZKOLE PUBLICZNE W ZEBRZYDOWICACH Zebrzydowice, ul. Makowa 1, 43-410 Zebrzydowice	1

7. Urządzenie wielofunkcyjne – 5 szt.

Parametr	Charakterystyka (wymagania minimalne)
Rodzaj urządzenia	Wielofunkcyjne – drukarka/skaner/kopiarka
Technologia druku	Laserowa monochromatyczna
Format	A4
Standardowa pamięć	512 MB
Rozdzielczość druku	600 x 600 dpi
Szybkość drukowania	Do 34 stron/min
Automatyczny druk dwustronny	Tak
Skanowanie w kolorze	Tak
Rozdzielczość skanowania	1200 x 1200 dpi (mono) 600 x 600 (kolor)
Skanowanie do plików	JPG, TIFF, PDF
Rozdzielczość kopiowania	600 x 600 dpi
Szybkość kopiowania	Do 30 stron/min
Pojemność podajnika papieru	Do 250 arkuszy
Obsługiwane formaty	A4, A5, A6, B5, Letter, Koperty

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Druk w sieci	Tak, przez LAN i WiFi
Rozwiązania komunikacyjne	USB, Ethernet, WiFi
Waga	Maksimum 10 kg
Obsługiwane systemy	Windows 8, 10, 11, MacOS 10.14, 10.15, 11
Gwarancja	Minimum 12 miesięcy

Użytkownik końcowy:	Ilość
SZKOŁA PODSTAWOWA W KACZYCACH Kaczyce, ul. Harcerska 13, 43-417 Kaczyce	2
SZKOŁA PODSTAWOWA IM. JAROSŁAWA DĄBROWSKIEGO W KOŃCZYCACH MAŁYCH Kończyce Małe, ul. Jagiellońska 56, 43-410 Zebrzydowice	1
SZKOŁA PODSTAWOWA W MARKLOWICACH GÓRNYCH Markłowice Górne, ul. Szkolna 25, 43-410 Zebrzydowice	1
SZKOŁA PODSTAWOWA IM. K.K.BACZYŃSKIEGO W ZEBRZYDOWICACH Zebrzydowice, ul. Jana Kochanowskiego 55, 43-410 Zebrzydowice	1

8. Dysk zewnętrzny (przenośny) USB - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ dysku	HDD
Format szerokości	2,5"
Pojemność dysku	2 TB
Interfejs dysku	USB 3.2 Gen.1
Złącze	USB Micro-B
Gwarancja	Minimum 2 lat gwarancji producenta lub autoryzowanego partnera producenta

Użytkownik końcowy:	Ilość
SZKOŁA PODSTAWOWA IM. JAROSŁAWA DĄBROWSKIEGO W KOŃCZYCACH MAŁYCH Kończyce Małe, ul. Jagiellońska 56, 43-410 Zebrzydowice	1

III. CZĘŚĆ III – OPROGRAMOWANIE

9. Oprogramowanie biurowe – 18 szt.

Zamawiający oczekuje dostawy 18 licencji dożywotnich oprogramowania **Microsoft Office LTSC Standard 2021 Edu** (oprogramowanie będzie użytkowane w szkołach) lub równoważnego (kryteria równoważności podano na końcu dokumentu OPZ) o następującej funkcjonalności:

- Edytor tekstu – Microsoft Word;
- Arkusz kalkulacyjny – Microsoft Excel;
- Program do przygotowania i prowadzenia prezentacji – Microsoft PowerPoint;
- Menedżer informacji osobistych i program komunikacyjny zapewniający ujednoczone miejsce do zarządzania pocztą e-mail, kalendarzami, kontaktami oraz innymi informacjami osobistymi i zespołowymi – Microsoft Outlook;
- Program przeznaczony do tworzenia i organizowania notatek – Microsoft OneNote;
- Program służący do tworzenia materiałów marketingowych – Microsoft Publisher.

Użytkownik końcowy oprogramowania:	Liczba licencji
SZKOŁA PODSTAWOWA IM. JAROSŁAWA DĄBROWSKIEGO W KOŃCZYCACH MAŁYCH Kończyce Małe, ul. Jagiellońska 56, 43-410 Zebrzydowice	10
SZKOŁA PODSTAWOWA W MARKLOWICACH GÓRNYCH Marklowice Górne, ul. Szkolna 25, 43-410 Zebrzydowice	5
GMINNE PRZEDSZKOLE PUBLICZNE W ZEBRZYDOWICACH Zebrzydowice, ul. Makowa 1, 43-410 Zebrzydowice	3

10. Oprogramowanie antywirusowe – 150 szt.

Licencja/Subskrypcja na okres 12 miesięcy.

Minimalne funkcjonalności oprogramowania:

Ochrona systemów przed szkodliwym oprogramowaniem i zagrożeniami z Sieci - założenia ogólne
1. Polska i angielska wersja językowa.
2. Pełne wsparcie dla systemów 32 bitowych i 64 bitowych.
3. Wspólny instalator pakietu dla systemów 32 bitowych i 64 bitowych kontrolujący niezbędne wymagania systemowe.
4. Możliwość stworzenia automatycznego instalatora pozwalającego na bezobsługową instalację pakietu z zadanymi parametrami.
5. Wielopoziomowy silnik antywirusowy wykrywający wszystkie rodzaje zagrożeń: <ul style="list-style-type: none"> – konie trojańskie, wirusy, exploity, backdoory itp.; – narzędzia hakerskie, aplikacje potencjalnie szkodliwe i niechciane; – aplikacje typu adware/spyware; – aplikacje ukrywające swoją obecność w systemie, rootkity.

6. Moduł pozwalający na pełne usunięcie wykrytych, niechciany aplikacji łącznie z wykorzystywanymi przez nie bibliotekami, sterownikami i wpisami w rejestrze systemowym.
7. Skanowanie wszystkich popularnych formatów archiwów i konwerterów (w tym kompresorów plików wykonywalnych).
8. Możliwość włączenia tzw. trybu gracza pozwalającego na pracę przy komputerze nie przerywaną ewentualnymi komunikatami programu - po włączeniu tego trybu program sam podejmuje decyzje w sytuacjach alarmowych.
9. Zaawansowane mechanizmy heurystyczne pozwalające na wykrywanie nieznanych jeszcze zagrożeń.
10. Możliwość indywidualnej zmiany ustawień poziomu heurystyki dla poszczególnych modułów ochronnych pakietu.
11. Dostęp do wszystkich wykrytych w systemie infekcji z poziomu głównego okna programu wraz z możliwością ich natychmiastowego usunięcia.
12. Zaawansowany skaner na żądanie.
13. Monitor antywirusowy kontrolujący wszystkie uruchamiane/otwierane/kopiuwane/zapisywane pliki nie pozwalający na dostęp do plików zainfekowanych/szkodliwych.
14. Moduł kontroli rodzicielskiej/kontroli dostępu pozwalający na wszechstronne kontrolowanie/blokowanie treści pobieranych z Internetu.
15. Skaner poczty kontrolujący pocztę przesyłaną protokołami POP3/SMTP/IMAP.
16. Ochrona przeglądarki kontrolująca wszystkie pobierane przez przeglądarkę dane.
17. Zapora sieciowa.
18. Moduł szyfrowanych dysków.
19. Menadżer haseł.
20. Moduł czyszczenia systemu ze zbędnych plików.
21. Moduł skanowania rejestru systemowego.
22. Zaawansowane mechanizmy ochronne oparte o chmurę obliczeniową producenta.
23. W pełni automatyczny mechanizm aktualizacji zarówno baz wirusów jak i modułów programu nie wymagający ingerencji użytkownika.
24. Zaawansowany mechanizm raportowania obejmujący wszystkie istotne z punktu widzenia funkcjonowania pakietu zdarzenia.
25. Możliwość zabezpieczenia hasłem konfiguracji pakietu.
26. Pomoc techniczna dla programu świadczona w języku polskim.
27. Możliwość zdalnego połączenia (za zgodą użytkownika) z komputerem klienta przez wykwalifikowanego pracownika wsparcia technicznego producenta w celu rozwiązania problemów wskazanych przez użytkownika.
28. Moduł Administracyjny do zdalnego zarządzania instalacjami pakietu w sieci z konsolą umożliwiającą zdalny dostęp do serwera zarządzającego.
29. Możliwość czasowej deaktywacji ochrony na wskazany czas albo do ponownego uruchomienia systemu.
30. Pełna obsługa systemów: <ul style="list-style-type: none"> - Windows XP SP3 z IE 8 - Windows Vista SP2 z IE 9 - Windows 7 SP1 z IE 11 - Windows 8 - Windows 8.1 - Windows 10

<ul style="list-style-type: none">– Windows 11– Windows Server 2003 SP2 z IE 8– Windows Server 2003R2 SP2 z IE 8– Windows Server 2008 SP2 z IE 9– Windows Server 2008R2 SP1 z IE 11– Windows Server 2012– Windows Server 2012R2– Windows Server 2016– Windows Server 2019– Windows Server 2022– Android 8.0 lub nowszy
Monitor antywirusowy/ochrona plików
1. Analiza wszystkich uruchamianych/otwieranych/kopiuowanych/pobieranych plików.
2. Mechanizm uniemożliwiający dostęp do zainfekowanych obiektów.
3. Możliwość definiowania akcji podejmowanych przez monitor w przypadku wykrycia szkodliwego pliku: <ul style="list-style-type: none">– Leczenie pliku (lub jego usunięcie w przypadku, gdy leczenie nie jest możliwe)– Kasowanie pliku– Przeniesienie pliku do kwarantanny– Pytanie do użytkownika - w tym wypadku program wyświetla okno z pytaniem o akcję, która ma zostać podjęta.
4. Możliwość natychmiastowego wysłania zainfekowanego pliku do producenta w celu jego dalszej analizy.
5. Możliwość włączenia/wyłączenia skanowania plików na zasobach sieciowych.
6. Możliwość zablokowania mechanizmów autostartu na nośnikach zewnętrznych (np. autorun.inf na nośnikach USB).
7. Możliwość definiowania listy plików i folderów wyłączonych z ochrony antywirusowej.
Skaner na żądanie
1. Możliwość skanowania wszystkich zasobów komputera.
2. Mechanizm szybkiego skanowania pozwalający na sprawdzenie najważniejszych zasobów komputera. Skanowanie szybkie może być uruchomione: <ul style="list-style-type: none">– Na żądanie– Po starcie systemu– Po zalogowaniu użytkownika– Po aktualizacji baz wirusów
3. Możliwość uruchomienia skanowania wybranych zasobów z poziomu menu kontekstowego (prawoklik)
Kontrola rodzicielska/Kontrola dostępu
1. Baza danych szkodliwych treści podzielona na kategorie pozwalająca na dostosowanie poziomu ochrony do wieku i wymagań użytkowników.
2. Możliwość definiowania reguł obejmujących strony dopuszczane i blokowane zarówno na podstawie adresów stron jak i na podstawie ich treści.
3. Możliwość włączenia trybu bezpiecznego wyszukiwania.
4. Możliwość zablokowania pobierania programów z Internetu.
5. Możliwość definiowania tygodniowego harmonogramu dostępu do Sieci.
6. Możliwość definiowania listy użytkowników wykluczonych z kontroli rodzicielskiej.

7. Dostęp do historii przeglądanych stron z możliwością natychmiastowego dodawania adresów z listy do bazy stron blokowanych lub dopuszczanych.
Ochrona przeglądarki
1. Skanowanie całego ruchu realizowanego za pośrednictwem przeglądarek internetowych niezależnie od ich wersji.
2. Skanowanie połączeń szyfrowanych HTTPS.
3. Możliwość definiowania listy domen wykluczonych ze skanowania.
4. Funkcja blokowania transmisji strumieniowych (audio/video).
5. Możliwość blokowania pobierania niepodpisanych plików wykonywalnych.
6. Zaawansowany mechanizm skanowania i analizy załączników pocztowych w ramach wszystkich popularnych serwisów pocztowych - gmail, onet, wp, tlen, microsoft itp.
Bezpieczna przeglądarka internetowa
1. Kontrola uruchomionych aplikacji.
2. Ochrona przed 'wstrzykiwaniem' bibliotek do przeglądarki.
3. Filtr antyphishingowy.
4. Kontrola przekierowania ruchu sieciowego.
5. Ochrona schowka systemowego.
6. Ochrona pliku 'hosts'.
Ochrona poczty
1. Skanowanie poczty przesyłanej protokołami POP3/SMTP/IMAP.
2. Skanowanie połączeń szyfrowanych SSL/TLS.
3. Skanowanie nie wymaga zmiany ustawień kont pocztowych (adres serwera/użytkownik itp.) i działa niezależnie od używanego klienta pocztowego.
4. Mechanizm wykrywający i zabezpieczający przed uruchomieniem/otworzeniem potencjalnie szkodliwych załączników w formacie popularnych dokumentów/skryptów/programów wykonywalnych.
5. Możliwość usunięcia zainfekowanych wiadomości lub obudowania ich w strukturze bezpiecznego załącznika.
6. Możliwość dołączania do wysyłanych maili stopki z informacją o ich przeskanowaniu pod kątem infekcji.
7. Moduł antyspamowy oparty o sztuczną inteligencję zaimplementowaną przez producenta z możliwością definiowania własnych reguł przez użytkownika opartą między innymi o historię korespondencji.
Zapora sieciowa
1. Kontrola całego ruchu sieciowego w kontekście adresów oraz aplikacji.
2. Możliwość tworzenia reguł zapory zarówno dla adresów/portów jak i aplikacji oraz folderów lokalnych.
3. Tryb pracy interaktywnej oraz cichej, opartej na już stworzonych regułach.
4. W trybie interaktywnym, dla nowych połączeń program podaje szczegółowe informacje dotyczące zarówno adresów i portów jak i aplikacji realizującej połączenie. Użytkownik może podjąć decyzję o blokowaniu/przepuszczeniu połączenia oraz utworzenia reguły dla połączeń późniejszych.
5. Możliwość wyłączenia kontroli zapory dla połączeń realizowanych w ramach sieci lokalnych.
6. Możliwość definiowania sieci lokalnych.
7. Możliwość wyłączenia kontroli zapory dla połączeń wychodzących.
8. Funkcja blokowania aktywności sieciowej skryptów.
Szyfrowane dyski

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

1. Możliwość tworzenia szyfrowanych dysków o wskazanej pojemności.
2. Ochrona dostępu do danych zapisanych na dysku za pomocą hasła.
3. Wygodna konsola pozwalająca na zarządzanie dyskami: <ul style="list-style-type: none"> – Tworzenie dysku z możliwością definiowania jego nazwy – Usuwanie dysku – Montowanie dysku – Zmiana litery przypisanej do dysku.
Menadżer haseł
1. Możliwość stworzenia zaszyfrowanej bazy pozwalającej na przechowywanie haseł.
2. Indywidualna baza haseł dla każdego użytkownika w systemie.
3. Możliwość załączania obszernych notatek do każdego wpisu w bazie.
4. Możliwość włączenia podwójnej ochrony bazy z wykorzystaniem dodatkowego pliku klucza.
Kontrola urządzeń USB
1. Filtrowanie wszystkich rodzajów urządzeń USB podłączanych do komputera.
2. Identyfikacja urządzeń na podstawie producenta/produktu/opisu/numeru seryjnego.
3. Możliwość tworzenia reguł dopuszczających/blokujących na podstawie identyfikatorów urządzeń.
4. Raporty o wykorzystywanych w sieci urządzeniach dostępne z poziomu konsoli administracyjnej.
5. Mechanizm automatycznego skanowania nośników USB podłączanych do komputera.
Kontrola aplikacji
1. Kontrola uruchamiania aplikacji w systemie na podstawie zdefiniowanych reguł.
2. Identyfikacja aplikacji na podstawie całych ścieżek oraz linii poleceń.
3. Zarządzanie kontrolą aplikacji z poziomu konsoli administracyjnej.
4. Szczegółowe raporty o uruchamianych aplikacjach.
Kontrola urządzeń multimedialnych
1. Filtrowanie aplikacji nawiązujących połączenia z kamerą lub mikrofonem.
2. Możliwość tworzenia reguł dla wybranych aplikacji.
Czyszczenie systemu ze zbędnych plików
1. Analiza obszarów systemowych (kosz, pliki tymczasowe).
2. Analiza plików zapisywanych przez najpopularniejsze przeglądarki internetowe (w tym historia przeglądanych stron).
3. Możliwość pracy z uprawnieniami użytkownika lub administratora systemu.
Ochrona w chmurze
1. Możliwość włączenia przez użytkownika mechanizmów wspierających ochronę systemu danymi pochodzącymi z chmury obliczeniowej producenta. <ul style="list-style-type: none"> – Anonimowa analiza reputacji pracujących w systemie aplikacji – Weryfikacja potencjalnych zagrożeń (skryptów, makr itp.) w chmurze obliczeniowej producenta.
Ochrona klasy EDR
1. Zaawansowana analiza nietypowego zachowania aplikacji na stacjach w różnych obszarach ich interakcji z systemem i z Siecią, wykorzystująca potencjał wszystkich modułów ochronnych pakietu.
Aktualizacja pakietu
1. Tryb automatycznej aktualizacji pobierający najnowsze bazy wirusów i moduły programu z serwerów producenta lub z repozytorium tworzonego u użytkownika.
2. Możliwość tworzenia indywidualnego harmonogramu aktualizacji.

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

3. Możliwość tworzenia repozytorium aktualizacji i udostępniania go w sieci innym komputerom z wykorzystaniem protokołu http lub zasobu lokalnego.
4. Możliwość odroczenia aktualizacji plików wykonywalnych i bibliotek pakietu.
5. Możliwość aktualizacji pakietu i baz wirusów w trybie offline (np. ze wskazanego nośnika wymiennego).
6. Współpraca z serwerami proxy.
Raporty
1. Program tworzy raporty obejmujące wszystkie istotne z punktu widzenia jego funkcjonowania zdarzenia: <ul style="list-style-type: none">– Wykryte infekcje oraz wykonane akcje– Zainfekowana poczta– Infekcje na stronach WWW– Zablokowane urządzenia multimedialne– Zablokowane urządzenia USB– Nowe połączenia analizowane przez zaporę sieciową– Zablokowane strony w ramach kontroli rodzicielskiej (raporty przyrostowe)– Aktualizacja pakietu– Utworzenie kopii zapasowej.
2. Mechanizm kasowania raportów starszych niż 30 dni.
3. Przeglądarka raportów oferująca dostęp do zdarzeń z wybranego dnia.
Narzędzia dodatkowe i bezpieczeństwo danych
1. Mechanizm aktywnej ochrony dokumentów i innych ważnych plików użytkownika pozwalający na odzyskanie utraconych danych np. w efekcie działania zagrożeń typu Tesla Crypt czy Crypto Locker, obejmujący również ochronę plików znajdujących się na zasobach sieciowych.
2. Własny menadżer procesów dający dostęp do najważniejszych informacji o uruchomionych w systemie aplikacjach oraz o ich reputacji w oparciu o dane pochodzące z chmury obliczeniowej producenta.
3. Moduł kwarantanny pozwalający na bezpieczne przechowywanie zainfekowanych lub podejrzanych plików.
4. Moduł pozwalający na tworzenie kopii zapasowych ważnych dla użytkownika plików, oferujący między innymi: <ul style="list-style-type: none">– Możliwość tworzenia wielu profili kopii zapasowych obejmujących wybrane przez użytkownika zasoby– Możliwość tworzenia pełnych kopii zapasowych lub kopii przyrostowych– Możliwość wygodnego definiowania harmonogramu tworzenia kopii zapasowych– Możliwość wygodnego odzyskiwania zarchiwizowanych danych z wybranej wersji kopii zapasowej– Możliwość tworzenia kopii zapasowych na dyskach sieciowych.
5. Mechanizm pozwalający na wygenerowania szczegółowego raportu o systemie z możliwością wysłania go do producenta w celu analizy potencjalnych problemów w systemie użytkownika.
6. Mechanizm generacji nośnika ratunkowego (płyta, pendrive) pozwalającego na awaryjne uruchomienie komputera w przypadku awarii systemu.
7. Mechanizm akceleracji aktualizacji systemów Windows.
8. Moduł kontroli parametrów pracy systemu (w tym zużycie procesora i pamięci oraz kontrola dysków fizycznych pod kątem ryzyka awarii i utraty danych).
Ochrona urządzeń mobilnych z systemem Android
1. Prosta instalacja za pomocą instalatora APK.

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

2. Skanowanie istotnych zasobów systemu pod kątem infekcji.
3. Wykrywanie aplikacji o potencjalnie zbyt wysokich uprawnieniach.
4. Automatyczne skanowanie pobieranych plików.
5. Automatyczna aktualizacja baz zagrożeń.
6. Możliwość wykorzystania zasobów chmury obliczeniowej do skanowania systemu.
7. Zarządzanie pakietem z poziomu konsoli administracyjnej.
Moduł administracyjny do zarządzania instalacjami pakietu w sieci
1. Serwer zarządzający niewymagających zewnętrznych mechanizmów bazodanowych.
2. Konsola administracyjna w postaci wygodnej aplikacji pozwalająca na zdalny dostęp do serwera zarządzającego.
3. Możliwość tworzenia rozbudowanej struktury grup i podgrup zarządzanych stacji.
4. Automatyczne tworzenie repozytorium aktualizacyjnego dla zarządzanych stacji.
5. Możliwość definiowania indywidualnych ustawień dla każdej grupy i stacji.
6. Blokada możliwości zmiany ustawień i aktywności modułów ochronnych przez użytkowników na stacjach roboczych.
7. Zaawansowany system zbierania i przeglądania raportów i informacji o zdarzeniach w sieci.
8. Zbiorcze informacje o infekcjach dla każdej grupy w zarządzanej strukturze.
9. Możliwość eksportu zdarzeń dla danej grupy (lub całej sieci) do pliku CSV.
10. Możliwość zdalnego uruchomienia skanowania i aktualizacji na stacjach.
11. Dostęp do listy uruchomionych procesów na zarządzanych stacjach.
12. Informacja o zasobach sprzętowych zarządzanych stacji (procesor/pamięć/napędy/wersja systemu operacyjnego).
13. Dostęp do informacji o oczekujących aktualizacjach systemów Windows na systemach w sieci.
14. Możliwość zdalnego podglądu pulpitu zarządzanych stacji.
15. Możliwość zdalnego podglądu miniatur pulpitu zarządzanych stacji w grupach.
16. Możliwość przeglądania listy stron odwiedzanych przez użytkowników zarządzanych stacji.
17. Kontrola liczby stanowisk w kontekście wykorzystywanej przez użytkownika licencji.
18. Możliwość zdalnego uruchomienia procesów na wybranych stacjach z uprawnieniami użytkownika lub systemu.
19. Możliwość zdalnego wyłączenia/ponownego uruchomienia/zablokowania wybranych stacji.
20. Możliwość zdalnego uruchomienia wybranych stacji (funkcja Wake-on-LAN).
21. Współpraca z serwerami proxy.
22. Możliwość prostego przeniesienia stacji do innego serwera zarządzającego bezpośrednio z poziomu konfiguracji w konsoli.
23. Możliwość wysyłania mailowych powiadomień zdarzeniach w sieci.
24. Możliwość wysyłania raportów o zdarzeniach do serwera Syslog.
25. Możliwość wysyłania z poziomu konsoli komunikatów do użytkowników.
26. Możliwość kontroli parametrów pracy systemów w sieci (w tym zużycie mocy procesora i pamięci oraz kontrola dysków fizycznych pod kątem ryzyka awarii i utraty danych).

Użytkownik końcowy oprogramowania:	Liczba licencji
SZKOŁA PODSTAWOWA IM. JAROSŁAWA DĄBROWSKIEGO W KOŃCZYCACH MAŁYCH Kończyce Małe, ul. Jagiellońska 56, 43-410 Zebrzydowice	100

SZKOŁA PODSTAWOWA W MARKLOWICACH GÓRNYCH Marklowice Górne, ul. Szkolna 25, 43-410 Zebrzydowice	50
---	----

11. Specjalistyczne oprogramowanie do blokowanie treści niebezpiecznych – 135 szt.

Licencja/abonament na okres 12 miesięcy

Wymagania funkcjonalne oprogramowania:

1. Filtrowanie niebezpiecznych stron internetowych w oparciu o aktualizowaną na bieżąco bazę danych adresów oraz słów kluczowych.
2. Blokowanie serwisów społecznościowych (Facebook, Twitter, Instagram itp.).
3. Filtrowanie stron zaszyfrowanych SSL (YouTube, Google, Facebook itp.).
4. Kontrola działania wyszukiwarek internetowych, m.in. możliwość zablokowania wyszukiwania obrazków/zdjęć.
5. Podział bazy stron na kategorie.
6. Automatyczna aktualizacja bazy stron przez Internet.
7. Możliwość dodawania własnych stron blokowanych oraz słów kluczowych.
8. Możliwość zdalnego podglądu ekranów uczniowskich.
9. Przechowywanie i udostępnianie historii zablokowanych oraz przeglądanych stron.
10. Tworzenie statystyk czasu przebywania na stronach internetowych oraz korzystania z aplikacji Windows.
11. Funkcja zdalnego pulpitu, czyli możliwość zdalnej pracy na komputerze uczniowskim, z poziomu komputera nauczyciela
12. Wymagane działanie w systemach operacyjnych Microsoft Windows: Vista, Windows 7, 8 oraz Windows 10

Użytkownik końcowy oprogramowania:	Liczba licencji
SZKOŁA PODSTAWOWA IM. JAROSŁAWA DĄBROWSKIEGO W KOŃCZYCACH MAŁYCH Kończyce Małe, ul. Jagiellońska 56, 43-410 Zebrzydowice	100
SZKOŁA PODSTAWOWA W MARKLOWICACH GÓRNYCH Marklowice Górne, ul. Szkolna 25, 43-410 Zebrzydowice	35

IV. CZĘŚĆ IV – OPROGRAMOWANIE SPECJALISTYCZNE

12. Specjalistyczne oprogramowanie do monitorowania stanowiska pracy, kompleksowe zarządzanie infrastrukturą IT, monitorowanie urządzeń sieciowych oraz ochrona przed utratą poufnych danych

Oprogramowanie musi zostać dostarczone z licencją wieczystą na 2 konsole administracyjne i 70 agentów monitorujących, z pełnym rocznym wsparciem technicznym (bezpłatne aktualizacje i pomoc techniczna), z możliwością przedłużenia okresu wsparcia w cyklach rocznych.

Funkcjonalność minimalna:

Zarządzanie zasobami
Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne
Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania
Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP
Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji
Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy
Odwzorowanie struktury organizacji w oparciu o Active Directory
Jednostronna synchronizacja komputerów oraz drukarek z AD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
Automatyczne skanowanie całości lub wybranych grup Active Directory oraz sieci
Mapowanie atrybutów obiektów AD do obiektów programu
Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)
Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
Utworzenie własnych typów elementów wyposażenia
Łączenie elementów wyposażenia w zestawy
Przypisywanie zasobu do wielu zestawów
Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia
Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach
Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
Przypisywanie sprzętu do konkretnych osób
Przypisywanie sprzętu do wybranej firmy
Automatyczne wyznaczanie 'Głównego użytkownika' komputera
Wiązanie wielu rekordów wyposażenia z użytkownikiem
Przypisywanie sprzętu do dowolnej lokalizacji
Definiowanie własnych, dowolnych atrybutów sprzętu
Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu'
Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia
Określanie loga firmy oraz użycia go na wydrukach
Grupowa zmiana domeny/grupy roboczej zasobu
Informacje o sprzęcie
Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu
Wykrywanie komputerów typu All-In-One

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF)
Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu
Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM
Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany
Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd.)
Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)
Odczyt informacji o module TPM
Odczyt D3Dscore z WinSAT
Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.)
Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu
Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika)
Automatyczne tworzenie zestawów: Komputer + Monitor
Automatyczne utworzenie zestawów: Komputer + drukarka lokalna
Automatyczne utworzenie zestawów: host + maszyny wirtualne
Automatyczne wykrywanie czy komputer jest maszyną wirtualną
Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform
Określanie informacji o wykorzystywanej wirtualizacji
Podgląd zestawów, do których należy zasób
Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami
Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu
Definiowanie szczegółowych informacji finansowych
Obsługa walut w danych finansowych
Definiowanie bazy dostawców sprzętu i oprogramowania
Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu)
Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta
Agent odczytuje identyfikator SID komputera
Określanie adresu interfejsu webowego urządzenia sieciowego
Określanie typu gwarancji dla zasobu
Określenie wpływu biznesowego wybranego zasobu
Tworzenie własnych typów gwarancji
Określanie ikony dla typów zasobów
Integracja z Dell API
Wyszukiwanie i identyfikacja duplikatów zasobów
Geolokalizacja komputerów z agentem
Raporty zasobów
Raport dodanych załączników
Automatyczne tworzenie historii zmian sprzętu
Raport zbiorczy historii zmian w sprzęcie
Ewidencja zdarzeń serwisowych

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Dodawanie notatek\komentarzy dla zdefiniowanych obiektów zasobów
Informacja na temat pojemności dysków twardych oraz wolnego miejsca
Wydruk\dodawanie jako załącznik protokołu przekazania\zwrotu\utylicacji sprzętu
Wydruk\dodawanie jako załącznik protokołu przekazania dla całego zestawu
Kreator szablonów wydruków WYSIWYG
Definiowanie dedykowanych profili protokołów
Zapisywanie protokołów podczas generowania jako załącznik do zasobu
Wydruk\dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia
Wydruk lub zapis do pliku raportów ze szczegółami sprzętu
Porównywarka wyników skanowania sprzętu
Dzienniki zdarzeń systemu Windows
Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu
Geolokalizacja komputerów z agentem
Zarządzanie zasilaniem
Zdalne włączanie i wyłączenie komputerów
Obsługa SecureOn przy WakeOnLan
Tworzenie harmonogramów wyłączenia i włączania komputerów
Wybór 5 trybów zamknięcia systemu: Blokada komputera, Uśpienie, Hibernacja, Wyłączenie, Restart
Możliwość anulowania /wyświetlenia komunikatu jeśli jest zalogowany użytkownik
Możliwość przerwania / odłożenia zadania na żądanie użytkownika
Raport zadań jednorazowych oraz harmonogramów
Funkcje dodatkowe
Zdalne wykonywanie skryptów (batch/powershell) - Obsługa zadań jednorazowych i cyklicznych
Wykonywanie zadań dla wszystkich komputerów
Edytor skryptów z funkcją kolorowania składni
Wykorzystywanie predefiniowanych skryptów
Import informacji o wyposażeniu z pliku CSV
Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL)
Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu)
Generowanie kodów paskowych, QR dla każdego elementu wyposażenia
Obsługa kodów QR
Archiwum zasobów
Przeniesienie utylizowanego wyposażenia do archiwum
Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego
Zarządzanie sprzętem przez aplikacje mobilną
Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu
Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych
Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej
Grupowa zmiana atrybutów
Personalizacja statusów zasobów

Zarządzanie oprogramowaniem
Licencje
Inwentaryzacja licencji
Automatyczne tworzenie licencji na podstawie kluczy produktów
Odczytu OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego
Import licencji z pliku tekstowego
Automatyczne generowanie historii zmian w licencji
Określanie statusu licencji
Tworzenie własnych atrybutów licencji
Tworzenie notatek oraz załączników w dowolnym formacie do licencji
Tworzenie licencji z poziomu rozliczenia audytu legalności
Tworzenie licencji z poziomu raportu kluczy licencji
Tworzenie zestawów licencji
Relacja licencji z użytkownikiem, firmą, działem, lokalizacją
Zmiana typu licencji dla wybranej grupy
Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe)
Przypisywanie licencji do komputera
Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.)
Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska
Definiowanie licencji przeznaczonych do przyszłego zakupu
Definiowanie kluczy seryjnych i przypisywanie do licencji
Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją
Określenie wpływu biznesowego wybranej licencji
Skanowanie oprogramowania
Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera
Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecenia skanów
Śledzenie zmian w stanie zainstalowanego oprogramowania
Zdalny skan komputerów (bieżący lub okresowy)
Zmiana priorytetu skanowania oprogramowania
Skan komputerów niepodłączonych do sieci
Wysyłanie wyników skanowania offline na serwer FTP (Audyt)
Przekazywanie konfiguracji wzorcowej dla skanera offline
Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania
Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy
Określanie masek plików dla publikacji elektronicznych (e-book)
Skan plików skompresowanych
Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
Wbudowane profile skanowania (np. profil wzorcowy)
Definicja własnych ustawień skanowania
Porównywanie wyników skanowania oprogramowania
Wykrywanie plików multimedialnych
Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)

Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI
Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie
Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych
Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta
Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (* , %)
Audyt oprogramowania
Rozliczanie pakietów aplikacji
Rozliczanie systemów operacyjnych
Rozliczanie licencji typu „Downgrade”, „Upgrade” oraz instalacji innego oprogramowania w ramach licencji
Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji.
Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)
Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę
Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)
Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji
Funkcje
Mechanizm informujący o nowej bazie wzorców oprogramowania
Definiowanie własnych wzorców oprogramowania
Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych
Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania
Wykrywanie kluczy/identyfikatorów programów
W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza
Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office
Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania
Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, klucze zainstalowanych aplikacji
Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd.
Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.
"Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)
Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi)
Zdalna dezinstalacja oprogramowania
Utworzenie harmonogramu dezinstalacji oprogramowania
Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania
Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Raport zainstalowanych aktualizacji systemu Windows
Kontrola wykorzystania sprzętu i oprogramowania
Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne
Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) - jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach
Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)
Określanie firmy do której należy użytkownik
Określanie przełożonego dla użytkownika
Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy).
Prezentacja 'statusu użytkownika' (Zatrudniony, zwolniony, itd.)
Zarządzanie stanowiskami użytkowników
Przeniesienie rekordu użytkownika do archiwum
Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika
Odczytywanie informacji o użytkownikach z Active Directory
Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
Podgląd zdjęcia przypisanego do użytkownika
Przypisywanie do użytkownika załączników (pliki)
Przypisywanie notatek do użytkownika
Ewidencja zdarzeń przypisanych do użytkowników
Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory
Raporty
Analiza aktywności użytkowników
Zabezpieczenie przed skryptami i urządzeniami klikającymi
Grupowanie danych według komputerów jeśli użytkownik wykorzystywał więcej niż jedno stanowisko
Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP)
Analiza przerw w pracy
Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)
Analiza aktywności mikrofonu oraz kamery
Analiza wykorzystania poszczególnych aplikacji w czasie
Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie
Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika
Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny).
Statystyki najczęściej wykorzystywanych aplikacji
Statystyki wykorzystania komputerów przez poszczególnych użytkowników
Statystyki aktywności użytkownika i grup użytkowników
Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin
Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników

Kontrola wydruków - Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)
Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)
Monitoring wydruków na drukarkach sieciowych
Monitoring użytkowników stacji terminalowych
Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)
Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca
Raport zbiorczy historii zmian w rekordach użytkowników
Funkcje
Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.
Autoryzacja nośników zewnętrznych na podstawie wykrytych urządzeń
Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych
Automatycznie budowana baza informacji o napędach zewnętrznych
Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)
Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD-ROM
Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Użytkownicy
Informacje o ostatnio zalogowanych osobach na stacjach klienckich
Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje
Komentowanie przerw pracy
Kategoryzacja przerwy w pracy na podstawie komentarza
Kontrola wykorzystania Internetu
Funkcje
Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)
Blokada stron internetowych dla protokołu http \ https (Chrome, Firefox, Opera, Edge, Chromium, Vivaldi)
Kategoryzacja stron internetowych
Import stron WWW z pliku lub ze schowka
Słowniki kategorii stron WWW
Blokada dostępu do witryn zgodnie z harmonogramem
Blokada trybu incognito w przeglądarce Google Chrome
Raporty
Raporty dotyczące aktywności użytkowników w Internecie oparte na kontaktach użytkowników
Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki)
Monitoring stron internetowych dla protokołu http \ https (Edge, Chrome, Firefox, Opera, Vivaldi)
Analiza liczby wejść na poszczególne strony lub domeny
Analiza odwiedzanych domen i stron
Raport informujący o plikach pobranych przez przeglądarki WWW

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Monitoring wysyłanych oraz pobieranych plików przez przeglądarki internetowe
Helpdesk
Obsługa
Rejestracja i obsługa zgłoszeń
Obsługa zgłoszeń w modelu Kanban
Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny)
Edycja zgłoszeń powiązanych w oknie zgłoszenia bieżącego
Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii
Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów
Opis zgłoszenia w formacie HTML
Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydent
Tworzenie notatek dla zgłoszeń
Zapisywanie wersji roboczej komentarza
Archiwizacja zgłoszeń
Monitoring czasu pracy nad incydem (time tracking)
Raport ewidencji czasu pracy nad zgłoszeniem
Informacja o czasie reakcji do podjęcia zgłoszenia
Dodanie prywatnego komentarza
Znaki @ oraz # pozwalają na wspomnianie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia
Dodanie załączników do incydentów, również do komentarza
Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie
Określanie uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów)
Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń
Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń
Wydruk historii zgłoszenia
Widok kalendarza (Planowanie rozwiązania incydentów)
Korelacja incydentu z elementem zasobów
Raport zbiorczy historii zmian
Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej
Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania
Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA
Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu
Określenie wpływu biznesowego wybranego zgłoszenia
Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń email
Duplikacja i replikacja zgłoszeń
Powiadomienia o liczbie nieprzeczytanych zgłoszeń
Automatyzacja obsługi zgłoszeń z wykorzystaniem utworzonych reguł
Konfiguracja
Architektura drzewa dla kategorii zgłoszeń

Tworzenie szablonów odpowiedzi
Cykliczne raportowanie Listy incydentów
Tworzenie własnych dodatkowych atrybutów dla zgłoszeń
Personalizowane szablony wiadomości email
Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydentu
Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (Deadline)
Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP)
Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox)
Obsługa wielu kont pocztowych (Import + notyfikację email)
Tworzenie własnych trybów oraz priorytetów incydentów
Personalizacja widoku raportu listy incydentów
Profile zgłaszających w helpdesk
Personalizacja kolorów statusów zgłoszeń
Automatyczne przypisywanie zgłoszeń do użytkowników
Weryfikacja wiadomości źródłowych pobieranych z serwera pocztowego
Konfiguracja maksymalnej wielkości załącznika
Moduł połączeń zdalnych
Operacje na plikach i katalogach
Zarządzanie procesami i rejestrem
Monitoring pracy wykonywanej na komputerze
Zdalny podgląd pulpitu wielu stacji (Funkcja Company Online)
Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji
Wysyłanie wiadomości do użytkowników
Uruchamianie na stacjach programów z wiersza poleceń Command Line
Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan
Wake-On-Lan pozwala na definicję portu oraz adresu komputera docelowego
Przejęcie kontroli nad stacją roboczą
Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego
Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie
Przejęcie kontroli nad komputerem bez zalogowanego użytkownika
Wysyłanie pytania o zgodę na zdalny dostęp lub wysyłania komunikatu z informacją o rozpoczęciu podglądu pulpitu
Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen
Obsługa wielu monitorów dla podglądu pulpitu
Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu
Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie
Połączenie pulpitem zdalnym w konfiguracji NAT-NAT
Zarządzanie usługami systemu Windows
Raport Sesje zdalnego pulpitu
Wybór adresu IP, na którym ma być zestawione połączenie DirectPC
Wybór portu, na którym klient nasłuchuje połączenia zdalnego
Wykorzystanie protokołu autorskiego lub MS RDP do połączeń zdalnych
Baza wiedzy
Wbudowana baza wiedzy

Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk
Kopiowanie artykułów
Edytor HTML
Osadzanie załączników w treści artykułów
Osadzanie multimediów w treści artykułów
Baza wiedzy pozwala na tworzenia artykułów prywatnych oraz publicznych
Szybkie kopiowanie wpisów bazy wiedzy
Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk
Artykuły bazy wiedzy mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów
Informacja o liczbie odsłon artykułu bazy wiedzy
Bezpośrednie linkowanie artykułów bazy wiedzy
SLA
Definiowanie planów umów SLA
Definiowanie czasu obowiązywania umów SLA
Definiowanie czasu pracy działów wsparcia technicznego
Definiowanie dni wolnych na podstawie kalendarza świąt i dni wolnych
Definiowanie czasów reakcji oraz realizacji zgłoszenia
Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji
Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie
Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną umową SLA
Centralne repozytorium załączników
Funkcje
Załączniki przechowywane w centralnym repozytorium
Utworzenie relacji załącznika z innymi elementami systemu 1 - N (jeden do wielu)
Dodawanie i modyfikacja załączników z poziomu innych zasobów
Załączniki typu: link, udział oraz plik
Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura
Historia zmian załącznika
Zarządzanie użytkownikami
Funkcje
Raportowanie aktywności pracy
Przeglądanie ostatnio zgłoszonych incydentów
Powiązanie użytkownika z licencją
Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów
Cykliczne, automatyczne generowanie raportów
Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze
Zgłoszenia dotyczące wniosków nieobecności użytkowników
Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności

Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika
Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory
Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępny nadane w module RODO
Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych
Planowanie dni wolnych w widoku kalendarza
Planowanie zastępstw podczas nieobecności
Raportowanie cykliczne
Użytkownicy
Raport historia sesji
Raport Nośniki danych
Raport Operacje na plikach
Raport wydruków
Raport użycia aplikacji
Raport odwiedzonych stron WWW
Raport Wysyłane pliki
Raport czasu pracy przy komputerze
Raport Bizlook
Zasoby
Raport historii zasobów
Raport informujący o nowych zasobach
Raport informujący o nadchodzących terminach w zasobach
Raport Zasoby zarchiwizowane
Raport Systemy Operacyjne
Podstawowe
Raport Informacje o autoryzowanych agentach
Oprogramowanie
Raport zainstalowanego oprogramowania
Raport Szczegóły plików
Helpdesk
Raport incydentów (Helpdesk)
Raport czasu pracy nad zgłoszeniem
Raport Czasu SLA
Automatyzacja
Lista dostępnych reguł
Ogólne
Zakończenie asysty serwisowej
Wygaśnięcie certyfikatu SSL
Kończące się licencje na agenta

Zapełniona baza danych
Zasoby
Brak połączenia od agenta
Brak wolnej przestrzeni na dysku
Ostrzeżenie od Windows Security Center
Zakończenie skanowania sprzętu
Dodanie zasobu
Zmiana zasobu
Usunięcie zasobu
Zakończenie okresu gwarancyjnego
Zakończenie umowy serwisowej
Powielenie zasobów
Oprogramowanie
Zmiana oprogramowania
Zakończenie skanowania oprogramowania
Zamknięcie audytu
Licencje
Dodanie licencji
Zmiana licencji
Usunięcie licencji
Wygaśnięcie licencji
Planowana wymiana licencji
Użytkownicy
Dodanie użytkownika
Zmiana użytkownika
Usunięcie użytkownika
Helpdesk
Dodanie zgłoszenia
Usunięcie zgłoszenia
Zmiana zgłoszenia
Lista dostępnych Akcji
Wykonywanie skryptu na podstawie zdefiniowanej reguły
Wysłanie powiadomienia w konsoli zarządzającej na podstawie zdefiniowanej reguły
Wysyłanie powiadomienia mailowego na podstawie zdefiniowanej reguły (inicjator zdarzenia, Administratorzy, konkretny użytkownik, rozwiązujący, zgłaszający, subskrybenci)
Modyfikacja zasoby / użytkownika / zgłoszenia - w zależności od reguły
Dodanie komentarza (dla reguł Helpdesk)
RODO
Funkcje

Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie
Wydruk raportów tabelarycznych: czynności przetwarzania, dostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie
Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia
Wstępne wypełnienie wniosków o zmianę dostępu
Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji
Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych
Archiwizacja zbiorów
Definiowanie czynności przetwarzania
Przypisywanie zbioru danych do czynności przetwarzania
Przydzielanie dostępów do czynności przetwarzania
Zapisywanie historii zmian wniosków o dostęp do zbiorów
Dodawanie historycznych dostępów oraz wniosków o dostęp
Filtrowanie użytkowników w raporcie Dostęp
Raporty
Raport zbiorczy Czynności przetwarzania
Raport zbiorczy Zbiory danych
Raport zbiorczy zinwentaryzowanych dostępów
Raport zbiorczy zinwentaryzowanych powierzeń
Raport zbiorczy zinwentaryzowanych dokumentów
Raport zbiorczy historii naruszeń bezpieczeństwa
Raport zbiorczy wniosków o dostęp
Raport zbiorczy Dostęp
Sygnalista
Funkcje
Tworzenie zgłoszeń w postaci anonimowej lub nieanonimowej
Usuwanie metadanych z załączników zgłoszeń
Usuwanie danych osobowych ze zgłoszeń
Podział interfejsu na publiczny oraz dla wewnętrzny
Dashboard podsumowujący wykorzystanie portalu sygnalisty
Przypisywanie rozwiązujących zgłoszenia sygnalistów w zależności od typu zgłoszenia lub jego źródła
Definiowanie własnych atrybutów, kategorii, trybów zgłoszeń oraz poziomów ryzyka
Definiowanie stron publicznych (dostępnych dla sygnalistów)
Obsługa wielu języków stron publicznych
Natywne wsparcie języka ukraińskiego
Definiowany limit załączników
Wyróżnienie zgłoszeń o przekroczonym czasie reakcji
Raporty
Raport zgłoszeń
Historia zmian

Statystyka zgłoszeń
Pozostały czas na przyjęcie zgłoszenia
Pozostały czas do zakończenia
Widżety: Kategorie zgłoszeń, Poziomy ryzyka, Tryby zgłoszeń, Statusy zgłoszeń, Ostatnio dodane
Portal Web
Funkcje
Wallboard - ekran zbiorczy prezentujący wybrane informacje z całego systemu
Dashboard każdego modułu z najważniejszymi informacjami w postaci widżetów
Rozbudowane filtry dla raportów tabelarycznych
Zarządzanie użytkownikami, agentami, zasobami, licencjami, działami, audytami
Konfiguracja portalu helpdesk, kont administracyjnych oraz organizacji
Raporty dla każdego modułu w formie tabelarycznej
Obsługa helpdesk oraz bazy wiedzy
Obsługa modułu RODO
Obsługa modułu automatyzacja
Obsługa modułu Sygnalista
Automatyczne logowanie przy pomocy aplikacji
Logowanie za pomocą poświadczeń domenowych (SSO)
Logowanie za pomocą konta AzureAD
Wydruk raportów tabelarycznych
Kontrola statystyk użytkowników
Menu szybkiego dodawania nowych elementów (użytkownik, nieobecność, zasób, licencja, zgłoszenie, artykuł bazy wiedzy, zbiór danych, czynność przetwarzania)
Przełączanie wersji językowej bez ponownego logowania do systemu
Nawigacja Breadcrumb
Funkcjonalności ogólne
Określanie praw dostępu do grup zasobów lub użytkowników
Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca")
Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem
Wersja angielska (en-US) interfejsu użytkownika
Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL
Swobodna migracja danych pomiędzy MS SQL i PostgreSQL
Zdalna instalacja i dezinstalacja agentów na stacjach roboczych
Odczytywanie struktury organizacji z Active Directory
Skaner sieci wykorzystywany do wykrywania nowych urządzeń
Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta
Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta
Automatycznie dodane komputery\użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory
Definiowanie nieograniczonej liczby użytkowników systemu
Określanie ról dla kont systemu: Administratorzy, Menadżerowie, Zarządcy, Pracownicy
Indywidualny login i hasło dla poszczególnych użytkowników

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Automatyczne logowanie do systemu
Zarządzanie uprawnieniami użytkowników - określanie dostępu do poszczególnych obiektów systemu (konkretny użytkownik, konkretny zasób) , możliwość ograniczenia operacji (wyświetlanie, tworzenie, edycja, usuwanie)
Określanie ról użytkowników - zarządzanie grupami
Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem
Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)
Zgodny z pracą w sieciach WLAN
Podgląd aktualnych zadań serwera
Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników
Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami
Wyszukiwanie danych w tabelach raportów
Dowolne definiowanie grup sprzętu i użytkowników
Tworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne
Definiowanie i zapamiętywanie własnych widoków
Eksport danych bezpośrednio do MS Excel
Budowa zestawień metodą drag'n'drop
Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów
Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server.
Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP
Mechanizm kompresji pakietów danych przesyłanych przez Agenta
Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery)
Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy)
Definiowanie konfiguracji serwera proxy dla połączenia Agent-Server
Mechanizm zdalnego pobierania bieżących aktualizacji do programu
Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej
Dostęp do bazy wiedzy systemu
Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)
Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia backupu bazy w trybie wsadowym
Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania
Personalizacja pakietu instalacyjnego agenta
Określanie polityki haseł dla systemu
Zmiana języka systemu podczas logowania
Określenie numeru BDO przy definiowaniu rekordu firmy
Opcja resetu hasła podczas logowania
Globalne wyszukiwanie obiektów w systemie
Utworzenie atrybutów jako lista/słownik
Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników
Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring
Wyszukiwarka ustawień w opcjach systemowych

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych)
Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie
Skanowanie lasu domen
Budowa personalizowanego pakietu instalacyjnego
Automatyczne zamknięcie konsoli zarządzającej po zakończeniu sesji
Logowanie do portalu Web za pomocą mechanizmu Single Sign On
Logowanie operacji kont serwisowych
Dodatkowe informacje
Wersja darmowa z ograniczeniem do 3 agentów oraz 3 użytkowników
Kreator instalacyjny ułatwiający wdrożenie systemu
Aplikacja Master\Server\ Agent w wersji x64
Rozproszona architektura systemu: Serwer, Master, Agent (Możliwa praca każdego z komponentów na różnych komputerach)
Praca w oparciu o MS SQL Server oraz MS SQL Express (2008/2012/2014/2016/2019 32/64 bit)
Praca w oparciu o PostgreSQL 10 lub nowszy
Obsługa systemów operacyjnych - Agent : Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, Windows 11
Obsługa systemów operacyjnych - Master : Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, Windows 11
Obsługa systemów operacyjnych - Serwer : Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, Windows 11
Wszystkie wykonywalne komponenty systemu są podpisane certyfikatem DigiCert Code Signing Certificates for Microsoft Authenticode (Digicert)
Sterowniki systemowe są podpisane certyfikatem Extended Validation (EV) Code Signing Certificate (GlobalSign) i mogą pracować w 64-bitowych systemach operacyjnych Microsoft Windows™.

13. Oprogramowanie do zarządzania backupem danych w systemach firmy REKORD

Lista funkcji, które muszą być realizowane przez oprogramowanie:

Zarządzanie bazami danych
Zarządzanie bazami danych odbywa się z poziomu wydzielonej aplikacji. Lista dostępnych funkcjonalności obejmuje:
<ul style="list-style-type: none"> • definiowanie przestrzeni roboczych, • definiowanie serwerów, • definiowanie serwerów bazodanowych Firebird oraz PostgreSQL, • tworzenie baz danych dla silników Firebird i PostgreSQL, • wykrywanie na zarejestrowanych serwerach nowych baz danych nieobjętych backupem oraz możliwość ich rejestracji, • tworzenie polityk i planów backupu dla zarejestrowanych serwerów oraz baz danych, • zarządzanie usługami bazodanowym działającymi zdalnie na serwerach Linux oraz Windows,

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

<ul style="list-style-type: none"> • wykonywanie backupów (Firebird, PostgreSQL), • odtwarzanie danych z backupów (Firebird, PostgreSQL), • prowadzenie i monitoring aktywnych zadań w systemie, • monitoring i powiadomienia dotyczące stanu backupu na zarządzanych serwerach, • wysyłka alertów na maila.
<p>Zarządzanie dostępem i użytkownikami</p> <p>Zarządzanie strukturą organizacyjną, użytkownikami oraz dostępem wydzielone jest do odrębnej aplikacji. Lista dostępnych funkcjonalności obejmuje:</p>
<ul style="list-style-type: none"> • wydzielony moduł do uwierzytelniania, • wydzielony panel administracyjny pozwalający na instalację w sieci niedostępnej dla zwykłych użytkowników, • osobna tożsamość użytkowników, niezależna od tożsamości bazodanowej, • jednolite zarządzanie danymi identyfikacyjnymi użytkowników - loginy, hasła, uprawnienia do aplikacji - lista użytkowników w wydzielonej bazie danych, • możliwość zdefiniowania wzorca danych przy tworzeniu użytkowników, • grupowe zakładanie użytkowników na podstawie danych zewnętrznych (np. z systemu kadrowego, pliku XLSX), • możliwość zdefiniowania dowolnej ilości profili haseł, • możliwość przypisania profilu haseł do użytkownika, • możliwość wymuszania zmiany hasła przy pierwszym (kolejnym) zalogowaniu do systemu, • możliwość ustawianie losowego hasła z powiadomieniem użytkownika przez email, • możliwość wymuszania zmiany hasła zgodnie ze zdefiniowaną częstotliwością, • możliwość zdefiniowania ograniczenia ilości zmian hasła przez użytkownika w okresie 30 dni, • możliwość blokowania i odblokowywanie konta użytkownika, • możliwość określenia liczby nieudanych prób logowania, po których użytkownik zostanie zablokowany, • wyszukiwanie użytkowników, • własny mechanizm uwierzytelniania oparty na protokole OpenID Connect, • uwierzytelnianie poświadczeniami domenowymi (integracja z Microsoft Active Directory), • uwierzytelnianie poświadczeniami Windows, • obsługa Single Sign-On (jednokrotne logowanie do wielu aplikacji), • uwierzytelnienie oparte o tokeny, • obsługa centralnej struktury organizacyjnej z pełną historią zmian i możliwością sprawdzania stanu na dany dzień, • możliwość obsługi wielu organizacji z osobnymi strukturami komórek organizacyjnych, • sterowanie dostępem do instancji aplikacji na poziomie organizacji, • możliwość dodania lub usunięcia pracownika w organizacji/komórce organizacyjnej, • obsługa grup użytkowników, • komórki organizacyjnych stają się automatycznie grupami użytkowników, • obsługa listy dostępnych instancji aplikacji, • identyfikacja instancji aplikacji poprzez identyfikatory, dozwolone adresy URL i obsługiwaną metodę uwierzytelniania, • uwierzytelnianie instancji modułów aplikacji poprzez dedykowane identyfikatory i klucze, • mechanizm ról do obsługi uprawnień, • obsługiwane role na poziomie organizacji:

<ul style="list-style-type: none">○ Administrator – pełne uprawnienia administracyjne,○ Administrator organizacji- pełne uprawnienia administracyjne w kontekście organizacji (dostępne jedynie dla użytkownika w organizacji root),○ Obsługujący organizację (możliwe do wykorzystania przez aplikacje zewnętrzne, dostępne jedynie dla użytkownika w organizacji root),○ Członek organizacji,
<ul style="list-style-type: none">● obsługiwane role na poziomie aplikacji:<ul style="list-style-type: none">○ Użytkownik instancji aplikacji – może pracować na instancji aplikacji w kontekście organizacji,○ Administrator instancji aplikacji – administruje całą instancją aplikacji,○ Administrator instancji aplikacji dla organizacji -administruje instancją aplikacji wieloorganizacyjnej w kontekście organizacji,
<ul style="list-style-type: none">● historia operacji związanej z aktywnością użytkownika:<ul style="list-style-type: none">○ wylogowanie,○ autoryzacja,○ uwierzytelnienie,○ błąd uwierzytelniania,○ błąd autoryzacji,○ zablokowanie użytkownika,○ zablokowanie z powodu osiągnięcia limitu nieudanych prób,○ logowania,○ odblokowanie użytkownika,○ autoryzacja dla zmiany hasła,○ aktywność użytkownika,○ brak autoryzacji z powodu zablokowania,
<ul style="list-style-type: none">● historia operacji wykonanych przez administratora:<ul style="list-style-type: none">○ dodanie, edycja, usunięcie komórki organizacyjnej,○ dodanie, edycja, usunięcie organizacji,○ dodanie, edycja, usunięcie użytkownika,○ edycja grupy użytkowników,○ nadanie profilu haseł użytkownikowi,○ nadanie użytkownikowi roli w organizacji,○ odblokowanie użytkownika,○ przeniesienie komórki organizacyjnej,○ przeniesienie organizacji,○ przypisanie użytkownika do grupy użytkowników,○ przypisanie użytkownika do komórki organizacyjnej,○ trwałe zablokowanie użytkownika,○ usunięcie grupy użytkowników,○ usunięcie komórki organizacyjnej,○ usunięcie profilu haseł użytkownikowi,○ usunięcie przypisania aplikacji do organizacji,○ usunięcie użytkownika,○ usunięcie użytkownika z grupy użytkowników,○ usunięcie użytkownika z komórki organizacyjnej,○ usunięcie użytkownikowi roli w organizacji,○ utworzenie grupy użytkowników,○ wygenerowanie i zmiana hasła użytkownika,

- zablokowanie użytkownika,
- zamknięcie komórki organizacyjnej,
- zamknięcie organizacji,
- zmiana hasła użytkownika,
- zmiana loginu użytkownika,
- zmiana ustawień globalnych.

Usługa wdrożenia:

Usługa wdrożenia może zostać zrealizowana zdalnie, a w jej zakresie powinny zawierać się przynajmniej:

- instalacja i konfiguracja systemu,
- szkolenie administratora z wdrożonego systemu.

Kryteria równoważności

Ilekcroć w opisie przedmiotu zamówienia wskazane zostały znaki towarowe lub pochodzenie towaru, Zamawiający dopuszcza rozwiązania równoważne:

- a. Jeśli w dokumentach składających się na opis przedmiotu zamówienia, wskazana jest nazwa handlowa firmy, towaru lub produktu, Zamawiający – w odniesieniu do wskazanych wprost w dokumentacji przetargowej parametrów czy danych (technicznych lub jakichkolwiek innych), identyfikujących pośrednio lub bezpośrednio towar bądź produkt – dopuszcza rozwiązania równoważne. Jako rozwiązania równoważne, należy rozumieć rozwiązania charakteryzujące się parametrami nie gorszymi od wymaganych;
- b. Zgodnie z art. 101 ust. 5 ustawy Prawo zamówień publicznych, Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W przypadku oferowania produktów równoważnych, Wykonawca zobowiązany jest dołączyć do oferty dokumenty (np. karty techniczne, wydruki ze strony internetowej i inne) potwierdzające, że produkty równoważne spełniają pod względem jakości oraz funkcjonalności wymagania wskazane przez Zamawiającego.

Kryteria równoważności dla Microsoft Windows Server Standard 2022:

Lp.	Warunek równoważności
1.	Współpraca z procesorami o architekturze x86-64.
2.	Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3.	W ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wyposażonym w 2 procesory.
4.	Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych).
5.	Pojemność obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego - co najmniej 4TB.
6.	Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu.
7.	Praca w roli klienta domeny Microsoft Active Directory.
8.	Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2012.
9.	Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).
10.	Zawarta możliwość uruchomienia roli serwera DNS.
11.	Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP).
12.	Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
13.	Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
14.	Zawarta możliwość uruchomienia roli serwera stron WWW.

Lp.	Warunek równoważności
15.	W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
16.	W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych.
17.	W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego - darmowe aktualizacje w ramach wersji systemu operacyjnego pobierane przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat).
18.	Wszystkie wymienione w tabeli parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

Kryteria równoważności dla Microsoft Windows Server 2022 External Connector

Licencja dołączona do serwera, która umożliwia dostęp do oprogramowania serwera nieograniczonej ilości użytkowników zewnętrznych. Użytkownicy zewnętrzni to użytkownicy, którzy nie są pracownikami firmy lub podmiotów stowarzyszonych, ani wykonawcami lub agentami w siedzibie firmy lub podmiotów stowarzyszonych.

Kryteria równoważności dla Microsoft Windows Server Essentials 2022

Lp.	Warunek równoważności
1.	System fabrycznie zainstalowany przez producenta serwera.
2.	Współpraca z procesorami o architekturze x86-64.
3.	Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
4.	W ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wyposażonym w 1 procesor oraz 10 rdzeni fizycznych.
5.	Pojemność obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego 128GB.
6.	Jednoczesny dostęp do oprogramowania i możliwość korzystania z niego może mieć maksymalnie 25 unikalnych użytkowników lub 50 unikatowych urządzeń bez konieczności dokupowania dodatkowych licencji.
7.	Praca w roli klienta domeny Microsoft Active Directory.
8.	Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2012.
9.	Zawarta możliwość uruchomienia roli serwera DNS.
10.	Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP).
11.	Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
12.	Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
13.	Zawarta możliwość uruchomienia roli serwera stron WWW.
14.	W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

Lp.	Warunek równoważności
15.	W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na jednej maszynach wirtualnych.
16.	W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego - darmowe aktualizacje w ramach wersji systemu operacyjnego pobierane przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat).
17.	Wszystkie wymienione w tabeli parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

Kryteria równoważności dla produktu Microsoft Windows 10 Pro i Windows 11 Pro

Równoważny inny system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

Lp.	Warunek równoważności
1.	Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykaniem na urządzeniach typu tablet lub monitorach dotykowych
2.	Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.
3.	Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.
4.	Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI.
5.	Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
6.	Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
7.	Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
8.	Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
9.	Wbudowany system pomocy w języku polskim.
10.	Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
11.	Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
12.	Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
13.	Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14.	Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15.	Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
16.	Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".

17.	Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
18.	Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
19.	Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
20.	Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
21.	Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
22.	Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
23.	Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
24.	Wbudowany mechanizm wirtualizacji typu hypervisor."
25.	Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
26.	Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
27.	Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
28.	Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do minimum 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
29.	Możliwość zdefiniowania zarządzanych aplikacji w taki sposób, aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
30.	Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
31.	Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
32.	Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
33.	Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
34.	Możliwość tworzenia wirtualnych kart inteligentnych.
35.	Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
36.	Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
37.	Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
38.	Mechanizmy logowania w oparciu o: <ol style="list-style-type: none"> a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard),

	c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN, e. Certyfikat/Klucz i uwierzytelnienie biometryczne.
39.	Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.
40.	Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.
41.	Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
42.	Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń.
43.	Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń.

Kryteria równoważności dla Microsoft Office LTSC Standard 2021 Edu

LP.	W ZAKRESIE MINIMALNYCH WYMAGAŃ DO PAKIETÓW BIUROWYCH WYKONAWCA ZAPEWNI:
1.	Wersję językową: pełną polską wersję językową interfejsu użytkownika.
2.	Posiadanie portalu pomocy technicznej (FAQ) w języku polskim.
3.	Dostępność do pełnej dokumentacji w języku polskim.
4.	Osobną dożywną licencją dla każdej instalacji pakietu biurowego.

Zamawiający uzna oprogramowanie biurowe za równoważne określone w przedmiocie zamówienia, gdy charakteryzować się będzie on parametrami funkcjonalnymi i wydajnościowymi nie gorszymi niż przedstawione niżej kryteria równoważności:

LP.	OFEROWANE OPROGRAMOWANIE BIUROWE POWINNO POSIADAĆ NASTĘPUJĄCE CECHY W ZAKRESIE MINIMALNYCH WYMAGANYCH FUNKCJONALNOŚCI DOTYCZĄCYCH EDYTORA TEKSTU OPROGRAMOWANIE ZAPEWNI:
1.	Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
2.	Wstawianie oraz formatowanie tabel.
3.	Wstawianie oraz formatowanie obiektów graficznych.
4.	Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
5.	Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
6.	Automatyczne tworzenie spisów treści.
7.	Formatowanie nagłówków i stopek stron.
8.	Sprawdzanie pisowni w języku polskim.
9.	Śledzenie zmian wprowadzonych przez użytkowników.
10.	Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
11.	Określenie układu strony (pionowa/pozioma).
12.	Wykonywanie korespondencji seryjnej, bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
13.	Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
14.	Poprawnie funkcjonujący z platformą edukacyjną Microsoft
	W ZAKRESIE MINIMALNYCH WYMAGANYCH FUNKCJONALNOŚCI DOTYCZĄCYCH ARKUSZA KALKULACYJNEGO OPROGRAMOWANIE ZAPEWNI:

Umowa o powierzenie grantu o numerze 3068/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00
Finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego

1.	Tworzenie raportów tabelarycznych.
2.	Tworzenie wykresów liniowych (wraz z linią trendu), słupkowych, kołowych.
3.	Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
4.	Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
5.	Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych, a także narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
6.	Tworzenie raportów tabeli przestawnych umożliwiającą dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
7.	Wyszukiwanie i zmianę danych.
8.	Wykonywanie analiz danych przy użyciu formatowania warunkowego.
9.	Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
10.	Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
11.	Formatowanie czasu, daty i wartości finansowych z polskich formatem.
12.	Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
13.	Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
14.	Poprawnie funkcjonujący z platformą edukacyjną Microsoft
W ZAKRESIE MINIMALNYCH WYMAGANYCH FUNKCJONALNOŚCI DOTYCZĄCYCH NARZĘDZIA DO PRZYGOTOWANIA I PROWADZENIA PREZENTACJI OPROGRAMOWANIE ZAPEWNIĄ:	
1.	Przygotowanie prezentacji multimedialnych, które będą prezentowane przy użyciu projektora multimedialnego.
2.	Drukowanie w formacie umożliwiającym robienie notatek.
3.	Zapisanie jako prezentacja tylko do odczytu.
4.	Nagrywanie narracji i dołączanie jej do prezentacji.
5.	Opatrywanie slajdów notatkami dla prezentera.
6.	Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
7.	Umieszczanie tabeli i wykresów pochodzących z arkusza kalkulacyjnego.
8.	Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
9.	Możliwość tworzenia animacji obiektów i całych slajdów.
10.	Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
11.	Poprawnie funkcjonujący z platformą edukacyjną Microsoft