Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Załącznik nr 8 do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Postępowanie prowadzone w trybie podstawowym na:

Zakup i dostawę sprzętu komputerowego i oprogramowania w ramach
Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V
Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU

Specyfikacja techniczna
dla części I – zakup i dostawa serwerów wraz z wyposażeniem serwerowni

1. Serwer 2 szt.

Lp	Parametr	Wartość wymagana
1	Obudowa	Obudowa Rack 19” o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych (szyny ruchome).Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
2	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
3	Procesor	Zainstalowany jeden procesor szesnasto-rdzeniowy klasy x86 wyposażony w min. 24MB CACHE, o taktowaniu min. 2.4 GHz
4	RAM	64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. Zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
5	Kontroler RAID	Sprzętowy, Pamięć cache 8 GB, Poziomy RAID 0/1/5/6/10/50/60, Rodzaje dysków 12Gb/s SAS, 6Gb/s SAS/SATA, 3Gb/s SAS/SATA, Wsparcie PCI PCIe Gen. 4
6	Dyski twarde	2x 960GB SSD vSAS Mixed Use, pojemność dysku 960GB, wymiary 2,5” w ramce 3,5”, typ dysku SSD vSAS MU SED, interfejs SAS 12GB, typ obudowy Hot-Plug. Możliwość Zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w dwa nośniki typu flash o pojemności min. 16GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. Pamięć flash musi pochodzić bezpośrednio od producenta serwera.
7	Optymalizacja rozruchu	BOSS 2 x 480GB R1 M.2 SATA
8	Interfejsy sieciowe	Wbudowane min. 2 interfejsy sieciowe 1Gb/s Ethernet w standardzie 1000Base-T oraz dodatkowo 2 interfejsy sieciowe o przepustowości 10Gb/s Ethernet w standardzie 10GBase-T (porty mogą być osiągnięte poprzez kartę w slotach PCIe)

9	Zasilanie	Min. 2 zasilacze Redundantne, Hot-Plug min. 750W każdy
10	Wbudowane porty	min. 2 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty RJ45, min. 1 port VGA. (Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x1200)
11	Warunki gwarancji	36 miesiące gwarancji, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w dni robocze w godzinach 9-16. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

2. Serwer NAS 1 szt.

Lp	Parametr	Wartość wymagana
I	Specyfikacja sprzętowa	
1	Procesor	Procesor 64 bit o taktowaniu nie mniejszym niż 1,7 GHz, liczba rdzeni min. 4 np. Procesor AlpineAL-314 lub lepszy
2	Pamięć RAM	Nie mniej niż 8GB DDR3 1600MHz
3	Obsługiwane dyski twarde	Min. 4 szt. 3.5" oraz 2.5"
4	Interfejsy sieciowe	RJ45 (LAN) 1 Gbps - 2 szt., SFP+ - 1 szt.
5	Porty USB min. 3.2	Minimum 4
6	Typ obudowy	RACK 1U, zasilacz wbudowany
II	Specyfikacja oprogramowania	
1	Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
2	Szyfrowanie wolumenów	Tak, min AES 256
3	Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Skanowanie uszkodzonych bloków (pliku) Obsługa migawek Obsługa replikacji migawek
4	Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci
5	Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows

6	**Darmowe aplikacje na urządzenia mobilne**	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
7	**Minimum obsługiwane serwery**	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer Monitoringu Serwer wydruku
8	**VPN**	VPN client / VPN server. Obsługa PPTP, OpenVPN
9	**Obsługiwane protokoły sieciowe**	AFP, Dynamiczny DNS (DDNS), HTTP, HTTPS, iPv4/iPv6, iSCSI, Klient protokołu BitTorrent, Klient VPN, Obsługa ramek typu jumbo, Serwer CIFS/SMB, Serwer DHCP, Serwer DLNA, Serwer FTP, Serwer iTunes, Serwer NFS, S.M.A.R.T., SNMP, SSH, Telnet
10	**Możliwość instalacji dodatkowego oprogramowania**	Tak, sklep z aplikacjami; możliwość instalacji z paczek

3. Dyski do serwera NAS 4 szt.

Lp	Parametr	Wartość wymagana
1	**Rodzaj urządzenia:**	Dysk twardy - wewnętrzny
2	**Pojemność:**	Min. 4 TB
3	**Rodzaj obudowy:**	3,5"
4	**Interfejs:**	SATAIII 6Gb/s
5	**Wielkość bufora:**	Min. 256 MB
6	**Cechy:**	Zwiększona odporność na drgania, Zgodność z systemami NAS, technologia konwencjonalnego zapisu magnetycznego (CMR)
7	**Prędkość obrotowa:**	7200 obr/min
8	**MTBF:**	Min. 1 000 000 godzin

4. Konsola KVM 1 szt.

Lp	Parametr	Wartość wymagana
1	**Rodzaj urządzenia:**	**Konsola modułowa KVM LCD 19”**
2	**Matryca:**	aktywna TFT LCD, 19" XGA, format 4÷3; Rozdzielczość maksymalna: 1920x1080; Rozdzielczość optymalna: 1280x1024; Kontrast: 1000 ÷ 1; Jasność: 250 cd/m2; Podświetlanie: LED; Liczba kolorów: 16,7 milionów; Średni czas bezawaryjnej pracy (MTBF): 100 000 godzin
3	**Rodzaj obudowy:**	Rack , 1U
4	**Liczba portów PC lub KVM:**	8 PS2 lub USB
5	**Klawiatura:**	101 klawiszy , Touchpad

6	Cechy:	Zasilanie: ~230V AC; Dopuszczana temperatura pracy: 0°C ÷ 50°C; Dopuszczalna wilgotność powietrza: 10% ÷ 90%, niekondensująca;; Min-max rozstaw szyn: 580mm - 870mm;
7	Certyfikaty:	CE
8	Gwarancja:	2 lata

5. Zasilacz awaryjny 3 szt.

Lp	Parametr	Wartość wymagana
1	Rodzaj urządzenia:	Zasilacz awaryjny On-line
2	Topologia:	On-line
3	Moc pozorna/skuteczna:	1000VA/800W
4	Napięcie wejściowe:	160-280 V
5	Gniazda wyjściowe	IEC 320 C13 3szt. USB, RS-232
6	Zabezpieczenia:	Przeciążeniowe, termiczne, przed przeładowaniem
7	Sygnalizacja pracy:	Wyświetlacz LCD, Dźwiękowa
8	Gwarancja:	2 lata

6. Switch 2 szt.

Lp.	Parametr	Wartość wymagana
1	**Porty Ethernet**	48 gigabitowy port PoE+ RJ45 Ethernet 10/100/1000 Mb/s
2	**Sloty SFP+ 10Gb/s**	Min. 4
3	**Port konsolowy**	RJ45 1szt. micro-USB 1szt.
4	**Porty PoE+ (RJ45)**	Porty PoE+: 48 portów, do 30 W na każdym porcie, budżet: 500 W
5	**Maksymalny pobór mocy**	50W (bez podłączonego urządzenia z obsługą PoE) 640W (podczas zasilania z mocą 500W)
6	**Obudowa**	RACK 1U
7	**Chłodzenie**	Min. 3 wentylatory
8	Gwarancja:	2 lata

Specyfikacja techniczna oferowanego sprzętu
dla części II – zakup i dostawa urządzenia wielofunkcyjnego A3 mono

1. Urządzenie wielofunkcyjne A3 mono 1szt.

Lp.	Parametr	Wartość wymagana
1	**Technologia druku**	technologia laserowa, czterobębnowa
2	**Format oryginału i kopii**	A6-A3
3	**Prędkość drukowania**	Min. 50 stron A4 / min.
4	**Obsługiwane rozdzielczości drukowania**	600 x 600 dpi oraz 1200x1200 dpi
5	**Czas wydruku pierwszej strony**	maks. 4,5 sek.
6	**Czas nagrzewania**	maks. 20 sek. od włączenia zasilania
7	**Kopiowanie wielokrotne**	od 1 do 9999 kopii
8	**Pamięć RAM**	min. 4 GB
10	**Dysk SSD lub HDD**	min. 64 GB
11	**Zoom**	25-400%
12	**Panel operatora**	Panel operatora wyposażony w kolorowy ekran dotykowy LCD, o przekątnej min. 10 cali, w języku polskim. Panel z płynna regulacją kąta nachylenia.
13	**Dupleks**	automatyczny, obsługa papieru 80-250 g/m2
14	**Podajnik dokumentów**	Automatyczny dwustronny, pojemność tacy podającej min. 140 ark. (A4, 80 g/m2)
15	**Podajniki papieru**	podajnik automatyczny min. 4 x 500 ark. (80 g/m2), obsługa papieru 60-300 g/m2 (w tym min. jeden obsługujący papier formatu A3); taca boczna na min. 150 ark. (A4, 80 g/m2), obsługa papieru A6-A3, 60-300 g/m2
16	**Odbiór wydruków i kopii**	Taca odbiorcza na min. 500 arkuszy (80 g/m2)
17	**Podstawa mobilna**	Dedykowana, podstawa producenta urządzenia, na kółkach.
18	**Język opisu strony**	PCL 6, Post Script Level 3 (dopuszcza się emulacje)
19	**Interfejsy**	USB 2.0, Ethernet 10/100/1000 Mb
20	**Funkcje skanowania**	skanowanie do PC, do e-mail, do FTP, TWAIN (sieciowy), do pamięci przenośnej USB, WIA, SMB, do skrzynki dokumentów
21	**Rozdzielczość skanowania**	600 dpi
22	**Prędkość skanowania kolorowego**	min. 80 str. / min. (A4, 300 dpi)
23	**Typy plików**	PDF, PDF/A, PDF szyfrowany, PDF kompresowany, JPEG, TIFF, XPS, Opcjonalnie: PDF przeszukiwalny, docx, xlsx, pptx
24	**Wymagania dodatkowe**	Urządzenie wyposażone w funkcję zgłaszania usterek bezpośrednio na panelu dotykowym urządzenia.
25	**Materiały eksploatacyjne jako wyposażenie standardowe (dostarczone w komplecie z urządzeniem)**	**Tonery:** w ilości, która zapewni wydrukowanie minimum 40 000 stron A4 (przy 5% pokryciu) **Bębny:** w ilości, która zapewni wydrukowanie minimum 600 000 stron A4. Dostarczone materiały muszą być nowe i nieużywane, oraz wyprodukowane przez producenta oferowanych urządzeń.
26	**Możliwość rozbudowy**	Podajnik papieru na min. 3000 ark. (A4, 80 g/m2)

		Standardowy faks klasy Super G3 Finiszer zszywający, min. 1 taca odbiorcza o pojemności min. 4.000 ark. (A4, 80 g/m2),
27	**Wymagania dodatkowe**	Oferent musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzenia wielofunkcyjnego - dokumenty potwierdzające dołączyć do oferty Certyfikaty ISO 9001:2008 i ISO 14001:2004, producenta oferowanego sprzętu - załączyć do oferty

Specyfikacja techniczna
dla części III – zakup i dostawa sprzętu komputerowego tj.: serwera domeny, oprogramowania do szyfrowania poczty, sprzętowych urządzeń autoryzacyjnych do systemu operacyjnego lub kontrolera domeny

Przedmiotem zamówienia jest dostawa serwera zarządzania komputerami przy pomocy kontrolera domeny wsparcie techniczne i prawo do aktualizacji na 2 lata wraz z oprogramowaniem oraz wdrożeniem

1. Sewer zarządzający 1szt. oraz Serwer zapasowy 1 szt.

Lp	Parametr	Wartość wymagana
I	Specyfikacja sprzętowa	
1	Procesor	Jeden procesor czterordzeniowy z obsługą instrukcji 64 bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie http://www.cpubenchmark.net/high_end_cpus.html. Procesor z obsługą wirtualizacji.
2	Pamięć RAM	min. 32GB dedykowane do pracy serwerowej
3	Obsługiwane dyski twarde	4 kieszenie HotSwap SATA3 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap.
4	Interfejsy sieciowe	Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s Wsparcie KVM przez LAN
5	**Typ obudowy**	RACK 1U, zasilacz wbudowany, Panel przedni chroniący kluczem dostępu do dysków, Czujnik otwarcia obudowy, Komplet szyn montażowych w zestawie
6	**Gwarancja**	2 lata gwarancji producenta
II	Specyfikacja oprogramowania	
1	**Zarządzanie systemem i konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność:**	interfejs obsługi serwera musi być realizowany przez najnowszą przeglądarkę internetową i być w standardzie Windows METRO, system powinien przed zalogowaniem do panelu zarządzającego informować w czasie rzeczywistym administratora o obciążeniu: całego systemu, procesora, pamięci oraz interfejsu sieciowego na dynamicznych wykresach. Wskazując myszką dane na wykresie powinny pokazywać wartość obciążenia. Informacje o obciążeniu całego systemu, procesora, pamięci oraz interfejsu sieciowego powinny być archiwizowane w serwerze i dostępne przez system raportujący dla okresów: godzinowy, dzienny, tygodniowy i miesięczny, serwer musi umożliwiać realizowanie usług (FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS), musi posiadać system antywirusowy, możliwość zarządzania serwerem poprzez protokół SNMP w wersji 1/2/3, musi umożliwiać dostęp administratorów przez przeglądarkę WEB, wbudowany firewall zarządzany przez przeglądarkę WEB,

		przed zalogowaniem administratora do interfejsu serwera WEB, powinien bez autoryzacji odczytywać parametry obciążenia serwera pokazywane na dynamicznych wykresach w przeglądarce WEB, system musi umożliwiać generowanie certyfikatów SSL przez przeglądarkę WEB, system powinien posiadać możliwość importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB,
2	**Obsługa domeny, dostarczone oprogramowanie musi zapewnić funkcjonalność:**	zarządzania do min. 50 użytkowników, grup, zarządzanie do min. 50 komputerów, zarządzanie do min. 50 urządzeń, zarządzania polisami GPO, obsługę profili użytkowników oraz profili mobilnych, obsługę do min. 75 jednoczesnych podłączeń do serwera domeny, zarządzania użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego przez przeglądarkę WEB, możliwość tworzenia użytkowników i grup w kontrolerze domeny przez przeglądarkę WEB, nadawania haseł dla użytkowników w kontrolerze domeny przez przeglądarkę WEB, wyszukiwania po nazwie użytkownika, grupy i komputera przez przeglądarkę WEB, listy użytkowników, którym wygasła ważność konta dostępna w przeglądarce WEB, listy zablokowanych kont w kontrolerze domeny dostępna w przeglądarce WEB, wszystkie operacje zakładania i modyfikacji oraz usuwania kont, grup, komputerów w kontrolerze domenowym przez przeglądarkę WEB powinny być raportowane w centralnym repozytorium systemowym, możliwość wyświetlenia oraz akceptowania polityki bezpieczeństwa przed zalogowaniem użytkowników do serwera domenowego, administrator podłączający się do kontrolera domeny musi mieć możliwość autoryzacji i logowania się do serwera domenowego przy pomocy jednego dostarczonego do serwera urządzenia sprzętowego token wykorzystujący port USB, Administrator zanim dokona logowania do kontrolera domeny przy pomocy urządzenia sprzętowego token może wyświetlić wewnętrzną politykę bezpieczeństwa informacji Urzędu. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny. Administrator wyciągając urządzenie autoryzacyjne token z portu USB będzie miał blokowany system operacyjny. Zastosowane urządzenie sprzętowe token powinno umożliwiać przypisywanie konkretnego komputera (wraz z logowaniem administrator do kontrolera domeny) do urządzenia sprzętowego token, Pamięć urządzenia sprzętowego token musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domeny, Urządzenie sprzętowe token musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0, Urządzenie sprzętowe token w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u, współpracy z klientami Windows 7,8,8.1,10 w wersji professional.
3	**Licencja kontrolera domeny dla zamawianego serwera głównego i zapasowego musi umożliwiać:**	łatwe przenoszenie i uruchomienie kontrolera domeny pomiędzy zamawianym serwerem głównym i zapasowym, łatwe uruchomienie kontrolera domeny w trybie awaryjnym (w ograniczonej funkcjonalności) na dowolnym serwerze posiadanego przez zamawiającego na czas naprawy zamówionego serwera głównego lub zapasowego.
4	**Oprogramowanie musi**	obsługę minimum cztero-rdzeniowego procesora,

	umożliwiać wirtualizację dowolnych systemów operacyjnych i musi realizować:	obsługę minimum 32GB RAM-u, obsługę vmware VMDK, obsługę minimum 10 instancji środowisk wirtualnych, zapis stanu maszyny wirtualnej tzw. snapshot, kopii stanu maszyny wirtualnej, emulacji wielu urządzeń np. kart sieciowych, kontrolerów SAS, dynamicznej alokacji pamięci na kontener danych współpracy z kontrolerami SATA, SCSI, tryb pracy sieciowej min NAT, tunel UD, Bridge oraz wielu interfejsów sieci, zarządzanie poprzez przeglądarkę WEB, archiwizacje uruchomionych maszyn wirtualnych.
5	**Migracja użytkowników lokalnych do serwera domenowego działającego w systemie Windows Vista,7,8,8.1,10,11 w wersji 32 i 64 bity w wersji professional z licencją bezterminową na użytkowanie musi umożliwiać przenoszenie do 75 użytkowników i musi realizować:**	automatyczne przenoszenie profili i ustawień użytkownika z konta lokalnego do konta domenowego, automatyczne przeniesienie dokumentów użytkownika z konta lokalnego do konta domenowego i nadanie odpowiednich uprawnień ACL, automatyczne przenoszenie uprawnień plikowych i rejestru z konta lokalnego do konta domenowego automatyczne przeniesienie lokalnej skrzynki pocztowej Microsoft Outlook i Thunderbird z domyślnej lokalizacji w koncie lokalnym do konta domenowego.
III	Specyfikacja wdrożenia	
1	**Wykonawca do wdrożenia oferowanych rozwiązań musi posiadać następujące osoby z uprawnieniami**	jedną osobę posiadającą uprawnienia Audytora Wiodącego ISO 27001:2013 i Audytora Wewnętrznego ISO 14001 i 50001 lub uprawnienia równoważne, jedną osobę posiadającą uprawnienia Audytora Wewnętrznego ISO 27001:2013 i MCSA SQL Server 2012 i MCSA Windows Server 2012 lub uprawnienia równoważne.
2	**W ramach wdrożenia wykonawca przeszkoli kadrę informatyczną Urzędu**	Osoba szkoląca musi posiadać uprawnienia Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne

2. Ilość: 50 urządzeń autoryzacyjnych do systemu operacyjnego lub serwera kontrolera domeny - TOKEN

Lp	Parametr	Wartość wymagana
1	Funkcjonalność i cechy użytkowe:	Uwierzytelnienie użytkowników do systemu operacyjnego lub serwera kontrolera domeny przy pomocy dedykowanego urządzenia sprzętowego , monitorowania logów uwzględniające: - logowanie do systemu (kto, kiedy) - wylogowanie/zablokowanie systemu (kto, kiedy) Użytkownik zanim dokona logowania do systemu operacyjnego przy pomocy urządzenia sprzętowego może wyświetlić zdefiniowaną przez administratora wewnętrzną PBI. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny. Użytkownik, który opuszcza stanowisko pracy będzie miał blokowany system operacyjny przez urządzenie sprzętowe. Pamięć urządzenia sprzętowego musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego. Możliwość autoryzacji do systemu operacyjnego lub kontrolera domeny dedykowanym PIN-em. Możliwość nadawania indywidualnego kodu PIN do urządzenia autoryzacyjnego TOKEN dla konta użytkownika w systemie operacyjnym lub kontrolerze domeny. Zastosowane urządzenie sprzętowe powinno umożliwiać przypisywanie konkretnego komputera do urządzenia sprzętowego. Narzędzie sprzętowe musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0 Urządzenie sprzętowe w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u, Współpraca z klientami Windows 7,8,8.1,11

3. *Ilość: 50 Licencji oprogramowania do szyfrowania wiadomości email technologią END TO END. Wsparcie techniczne i prawo do aktualizacji na 2 lata. Bazy reguł, sygnatur i zagrożeń phishing na 2 lata.*

Lp	Parametr	Wartość wymagana
1	**Oprogramowanie musi zapewnić funkcjonalność**	szyfrowanie algorytmem AES256: treści wiadomości, załączników, plików, katalogów, do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu internetowego. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe. do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego. do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego. odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11,Ubuntu Desktop 20.04.3 ,Ubuntu Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0 szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania, opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność, zabezpieczenia każdego emaila dedykowanym unikalnym hasłem,

		posiadania wewnętrznej bazy haseł, która umożliwia: - export haseł do pliku, - import haseł z pliku - generowania ponownie haseł w bazie posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich, posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym, posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych, plików i katalogów, pracy i pomocy zdalnej użytkownikom poprzez przejęcie zdalnego pulpitu również poza siecią lokalną z użyciem jednorazowych wygenerowanych kodów autoryzacyjnych. Dodatkowo system pracy zdalnej musi działać niezależnie od włączonej funkcji UAC w systemie Windows. integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym, zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe, wykrywania fałszywych emaili - Antiphishing, wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING, wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych, wykrywanie niebezpiecznych dokumentów MS Office, wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email, definiowania alarmów informujących o niebezpiecznych mailach i załącznikach, współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 2 lata. Baza reguł, sygnatur i zagrożeń phishingowych powinna posiadać min. 1 500 000 wpisów. Producent musi umożliwiać wyświetlenie ilości wpisów na aktualny dzień poprzez stronę Internetową. Wpisy do bazy muszą być weryfikowane min. 2 razy w ciągu dnia, alarmowanie o wybranych zagrożeniach phishingowych min. raz na miesiąc, współpracy z klientem Mozilla Thunderbird i Mozilla Thunderbird Portable dla systemów 32 i 64 Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11.
2	**Licencja**	Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy.
3	**Współpraca z oprogramowaniem antywirusowym**	Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy. Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami. ogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.
4	**Szkolenia**	Przeprowadzenie cyklicznych zdalnych szkoleń minimum raz w roku z tematyki cyberbezpieczeństwa, zagrożeń poczty email, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne przez 2 lata.

Specyfikacja techniczna
dla części IV – zakup i dostawa oprogramowania do zarządzania infrastrukturą IT

Ilość: 50 licencji

Parametr	Opis
	Oprogramowanie posiada budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciuszyfrowanego protokołu TLS 1.2. Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program wykorzystuje darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystaniaz Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., są odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innychkont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostępdo Opcji programu oraz logów działań innych administratorów. Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog.
MONITOROWANIE INFRASTRUKTURY	**(BEZAGENTOWO)** obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie: - wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping - wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU) - wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci - wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki - wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym koloremtła. - wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jakotła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku

	- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze - wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie - wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny - zablokowania mapy urządzeń przed przypadkową edycją - serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów - serwerów pocztowych: - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail,SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem) - program ma możliwość wykonywania operacji testowych - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa - monitorowania serwerów WWW i adresów URL - cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS - obsługi szyfrowania SSL/TLS w powiadomieniach e-mail - obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID - obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych - monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych - ruchu sieciowego - podłączonych stacji roboczych – graficzna prezentacja panelu switcha - ruchu generowanego przez podłączone do portów stacje robocze - serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie - wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia,czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu - wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturąurządzeń w przedsiębiorstwie (Oddziały) oraz

	tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatoraplików MIB, który umożliwia dodawanie definicji dla modułów SNMP. Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciąguprzyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzeniez listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurowaćautomatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut.Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMSz wykorzystaniem protokołu netGSM (SOAP).
W ZAKRESIE INWENTARYZACJI	Program automatycznie gromadzi informacje o sprzęcie i oprogramowaniuna stacjach roboczych oraz: 1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. 2. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 3. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. 4. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej:instalacji/deinstalacji aplikacji, zmian adresu IP itd. 5. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. 6. Umożliwia odczytanie numeru seryjnego (klucze licencyjne). 7. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 8. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 9. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanychplików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 10. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działaniaadministratorów wykonywane w tej funkcji są logowane.

	Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętui programowania: 1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, 2. tworzenia powiązań między zasobami a urządzeniami, 3. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, 4. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, 5. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości. Dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mailo zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, 6. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, 7. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, 8. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, 9. importu danych z zewnętrznego źródła (.CSV) 10. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan fakturyzakupu, gwarancji, dowolnego dokumentu itp., 11. tworzenia powiązań między zasobami a dokumentami w relacji 1:N, 12. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., 13. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanieczynności, 14. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, 15. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, 16. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, 17. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, 18. archiwizacji i porównywania audytów zasobów, 19. tworzenia kodów kreskowych dla zasobów, 20. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dlazasobów, które posiadają numer inwentarzowy, 21. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, 22. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), 23. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie

	wygaśnie licencja/gwarancja”). Dodatkowo dostępny jest Agent inwentaryzacji na system Android. Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: 24. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 25. Informacje o aplikacjach używanych w organizacji. 26. Tworzenie własnych wzorców aplikacji. 27. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 28. Informacje o komputerach, na których aplikacja została wykryta. 29. Zarządzanie posiadanymi licencjami. 30. Wskazywanie osób odpowiedzialnych za licencję. 31. Wskazanie użytkowników licencji. 32. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 33. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu, 34. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczbyposiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. 35. Zarządzanie posiadanymi licencjami: raport zgodności licencji. 36. Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe posiadają możliwość filtrowania elementów per oddział.
W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW	program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie: -Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), -Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach, -Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, -Informacji o edytowanych przez użytkownika dokumentach, -Historii pracy (cykliczne zrzuty ekranowe), -Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt), -Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), -Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dlakażdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki

	dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków, -Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail. Program ponadto posiada możliwość: -blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowaniawyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. -blokowania ruchu na wskazanych portach TCP/IP, -blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, -wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, -przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu(który można dołączyć np. do akt pracownika), -definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.
Pomoc zdalna	W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika.W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten zawiera również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat pozwala na: - zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lubdostęp ograniczony wyłącznie do pomocy technicznej

	- rozmowy również między „zwykłymi" użytkownikami - przesyłanie plików między rozmówcami w trybie online - tworzenie pokojów tematycznych, rozmów grupowych - oznaczanie kontaktów jako „ulubionych" na liście kontaktów - uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWWheldpesku - może być wyświetlany w trybie jasnym lub ciemnym W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany wtrybie jasnym lub ciemnym. Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępuprzez każdego pracownika. Moduł pomocy zdalnej umożliwia również: - pobieranie listy użytkowników z Active Directory, - zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, - zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowanysystem zarządzania regułami widoczności zgłoszeń, - tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, - automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, - procesowanie zgłoszeń użytkowników z wiadomości e-mail, - tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, - wykonywanie operacji na wielu zgłoszeniach równocześnie, - dołączanie załączników do zgłoszeń, - rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, - szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, - wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie wkreatorze wyświetlanym przy zamykaniu zgłoszenia, - zrzuty ekranowe (podgląd pulpitu), - dystrybucję oprogramowania przez Agenty,

	- dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), - zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacjinastępuje kolejkowanie zadania dystrybucji pliku, - możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz zpowiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, - planowanie nieobecności pracowników helpdesk, - obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, - generowanie raportów obsługi helpdesk, - zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), - zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), - wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.
MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM	**MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM** poprzez blokowanie urządzeń. 1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjściaoraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyskiprzenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia(drukarka, klawiatura, mysz itp.) mogą być podłączane. 5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwościąograniczenia alarmów tylko do nośników niezaufanych. 6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresieodczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 9. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.Zarządzanie prawami dostępu do rządzeń: 1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. -urządzenia prywatne są blokowane. 3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

	Audyt operacji na plikach na urządzeniach przenośnych: 1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. Podłączenie/odłączenie urządzenia przenośnego. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.