Załącznik nr 1b do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest realizacja założeń projektu Cyfrowa Gmina realizowane w ramach umowy o powierzenie grantu o numerze 1137/1/2021 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.

Zamawiający zastrzega sobie możliwość wezwania Wykonawcy, którego oferta została najwyżej oceniona, do okazania zaoferowanego oprogramowania, w celu sprawdzenia ich zgodności z wymaganiami określonymi przez Zamawiającego w SWZ.

Okazanie nastąpi w dniu wyznaczonym przez Zamawiającego, po terminie składania ofert. Zamawiający poinformuje o terminie przeprowadzenia okazania z co najmniej pięciodniowym wyprzedzeniem (dni kalendarzowe). Niestawienie się Wykonawcy w wyznaczonym czasie i miejscu na okazaniu (prezentacji) oprogramowania, uznane będzie jako negatywny wynik okazania, tj. niepotwierdzenie przez Wykonawcę wymagań określonych przez Zamawiającego, co będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt. 5 Ustawy Pzp.

Część II - Oprogramowanie do monitoringu komputerów

1. Oprogramowanie do monitoringu komputerów

Specyfikacja Techniczna Oprogramowania	
1.	**Oprogramowanie winno posiadać budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów dla 30 jednostek komputerowych.** **Oprogramowanie musi posiadać wsparcie producenta na okres min. 12 m-cy wraz z zapewnionymi darmowymi aktualizacjami oprogramowania.**
2.	Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana ma być co najmniej przy użyciu szyfrowanego protokołu TLS 1.2.
3.	Moduły mają umożliwiać kompleksową monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.
4.	Program winien mieć możliwość wykorzystywania darmowego silnika bazy danych z kodem źródłowym dostępnym na licencji open-source (np. PostgreSQL w wersji 12) dzięki czemu nie jest objęty limitem ilości danych.
5.	Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., mają być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Mają być również grupowane w osobnym, dedykowanym oknie. Pozwali to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.
6.	Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty ma być 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 mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą

	administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów.
7.	Program ma posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta.
8.	Działania administratorów mają być automatycznie eksportowane do zewnętrznego kolektora Syslog.
MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) **ma zawierać:**	
9.	Monitorowanie obejmować ma serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle
10.	Wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
11.	Wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
12.	Wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
13.	Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
14.	Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku.
15.	Wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze.
16.	Wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie.
17.	Wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny.
18.	Zablokowania mapy urządzeń przed przypadkową edycją.
19.	Serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program ma monitorować czas ich odpowiedzi i procent utraconych pakietów.
20.	Serwery pocztowych monitorowane w zakresie: • czas logowania do serwisu odbierającego oraz czas wysyłania poczty, • 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),

	• wykonywania operacji testowych, • wysłania powiadomienia jeśli serwer pocztowy nie działa.
21.	Monitorowanie serwerów WWW i adresów URL.
22.	Cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.
23.	Obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
24.	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.
25.	Obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.
26.	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.
27.	Serwisy Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie /zatrzymanie /zrestartowanie.
28.	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.
29.	Wydajności systemów Windows: • obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
30.	Program ma posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Program ma posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.
31.	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 przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.

32.	Integracja programu ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).
	W ZAKRESIE INWENTARYZACJI
33.	Program ma automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp., zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
34.	Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwi audytowanie i weryfikację użytkowania licencji w organizacji.
35.	Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
36.	Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
37.	Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
38.	Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
39.	Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
40.	Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
41.	Umożliwia wymianę plików do i ze stacją roboczej poprzez funkcję Menedżera plików.
42.	Działania administratorów wykonywane w tej funkcji są logowane.
43.	Moduł inwentaryzacji zasobów ma umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania: • przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, • tworzenia powiązań między zasobami a urządzeniami, • tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,

	• wskazania osób uprawnionych do użycia zasobów, • definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości dla danego urządzenia lub oprogramowania możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, • wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, • określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, • określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, • definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, • importu danych z zewnętrznego źródła (.CSV), przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., • tworzenia powiązań między zasobami a dokumentami w relacji 1:N, • oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., • ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, • generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, • przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, • konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, • konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, • archiwizacji i porównywania audytów zasobów, • tworzenia kodów kreskowych dla zasobów, • drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, • 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, • inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),

	• definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).
44.	Dodatkowo ma być dostępny Agent inwentaryzacji na system Android.
45.	Inwentaryzacja oprogramowania ma zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: • Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. • Informacje o aplikacjach używanych w organizacji. • Tworzenie własnych wzorców aplikacji. • Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. • Informacje o komputerach, na których aplikacja została wykryta. • Zarządzanie posiadanymi licencjami. • Wskazywanie osób odpowiedzialnych za licencję. • Wskazanie użytkowników licencji. • Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. • Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. • Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. • Zarządzanie posiadanymi licencjami: raport zgodności licencji. • Możliwość przypisania do programów numerów seryjnych, wartości itp.
46.	Okna audytowe mają posiadać możliwość filtrowania elementów per oddział.
	W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW
47.	Program ma umożliwiać 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 dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek.
48.	Program ma mieć możliwość monitorowania kosztów wydruków, nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.
49.	Program ma mieć możliwości: • blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen 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.
50.	Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
51.	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.
52.	Program ma posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania

	oraz blokowania aplikacji i stron internetowych.
MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM zapewniająca:	
53.	Blokowanie urządzeń i nośników danych.
54.	Program zarządza prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
55.	Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
56.	Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
57.	Blokownie ma dotyczyć tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
58.	Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
59.	Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
60.	Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
61.	Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
62.	Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.
Zarządzanie prawami dostępu do urządzeń	
63.	Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
64.	Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. • urządzenia prywatne są blokowane
65.	Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
66.	Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
67.	Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.
Audyt operacji na plikach na urządzeniach przenośnych	
68.	Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

69.	Podłączenie/odłączenie urządzenia przenośnego.
Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika	
70.	Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.
WSPIERA ZARZĄDZANIE CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW	
71.	Dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji ma mieć możliwość oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Ma mieć możliwość uzyskania dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mają mieć możliwość uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik ma mieć możliwość przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły mają umożliwić zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp realizowany ma być przez przeglądarkę internetową a strona może być wyświetlana w trybie jasnym lub ciemnym.
72.	Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
73.	Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
74.	Statystyki aktywności podwładnych widoczne dla przełożonego.
75.	Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
76.	Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
77.	Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
78.	Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
79.	Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
80.	Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
81.	Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
82.	Wskaźnik czasu poświęconego na aktywność produktywną.
83.	Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
84.	Możliwość przypisywania kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z

	możliwością edycji.
85.	Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.
86.	Program ma być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
87.	Ma istnieć możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.
88.	Program dostępny ma być w języku polskim, angielskim wraz z Podręcznikiem Użytkownika w formie strony internetowej.