OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa licencji systemu do zarządzania infrastrukturą IT (inwentaryzacja sprzętu i oprogramowania, audyt legalności, kontrola stanowisk, helpdesk, RODO, sygnalista) wraz ze wsparciem producenta oraz usługą wdrożenia w dwóch niezależnych sieciach IT i OT

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa licencji bezterminowych na oprogramowanie do kompleksowego zarządzania infrastrukturą IT (dalej: „System"), obejmujące inwentaryzację sprzętu i oprogramowania, zarządzanie licencjami i audyt legalności oprogramowania, kontrolę wykorzystania stanowisk komputerowych i nośników zewnętrznych, obsługę zgłoszeń (helpdesk), ewidencję w zakresie RODO oraz obsługę zgłoszeń sygnalistów, dla dwóch niezależnych instancji – w sieci IT oraz w sieci OT Zamawiającego – wraz ze wsparciem producenta oraz usługą wdrożenia.

1.2. W skład przedmiotu zamówienia wchodzą:

Lp.	Element przedmiotu zamówienia	Ilość
1.	Licencje bezterminowe na System – instancja dla sieci IT, w zakresie funkcjonalności z sekcji A–P tabeli w rozdz. 3	**20** stanowisk (agentów) **1** licencji konsoli administracyjnej
2.	Licencje bezterminowe na System – instancja dla sieci OT, w zakresie funkcjonalności z sekcji A–C, F, H, I, L–P tabeli w rozdz. 3	**20** stanowisk (agentów) **1** licencji konsoli administracyjnej
3.	Wsparcie producenta (asysta serwisowa) dla obu instancji – zgodnie z rozdz. 4	24 miesiące
4.	Usługa wdrożenia Systemu w dwóch niezależnych sieciach IT i OT wraz z instruktażem administratorów	1 usługa

1.4. Instancje dla sieci IT i OT muszą działać jako dwa całkowicie niezależne systemy, zgodnie z pkt 2.8 i rozdz. 5. Wymagania z rozdz. 3 dotyczą każdej z instancji w zakresie sekcji wskazanych dla niej w pkt 1.2.

1.5. Kod CPV: 48780000-4 Pakiety oprogramowania do zarządzania systemem, pamięcią i treścią; 48900000-7 Różne pakiety oprogramowania i systemy komputerowe; 72268000-1 Usługi dostawy oprogramowania; 72265000-0 Usługi konfiguracji oprogramowania.

2. Wymagania ogólne

2.1. Licencje muszą być licencjami bezterminowymi (udzielonymi na czas nieoznaczony), wystawionymi na Zamawiającego, obejmującymi liczbę stanowisk (agentów) oraz licencji konsoli administracyjnej wskazaną w pkt 1.2. Licencje nie mogą ograniczać liczby użytkowników Systemu (operatorów, zgłaszających), zasobów ewidencjonowanych bez agenta, zgłoszeń helpdesk ani wpisów w module RODO i Sygnalista.

2.2. Po zakończeniu okresu wsparcia producenta każda z instancji musi nadal działać w pełnym zakresie funkcjonalnym, z wykorzystaniem ostatniej zainstalowanej wersji oprogramowania, bez konieczności ponoszenia dodatkowych opłat.

2.3. System musi być instalowany w infrastrukturze Zamawiającego (on-premise), w środowisku wirtualizacyjnym Zamawiającego, odrębnym dla sieci IT i dla sieci OT. Działanie Systemu, w tym aktywacja licencji, nie może wymagać stałego połączenia z usługami chmurowymi producenta. Instancja OT musi zapewniać pełną funkcjonalność w środowisku bez dostępu do Internetu, z możliwością aktualizacji oprogramowania i bazy wzorców oprogramowania w trybie offline.

2.4. Funkcje wykorzystujące zewnętrzne usługi chmurowe (w szczególności funkcje AI, integracja z usługą modelu językowego, chmurowe skanowanie plików, geolokalizacja) muszą być domyślnie wyłączone lub możliwe do całkowitego wyłączenia przez administratora, tak aby żadne dane nie były przekazywane poza infrastrukturę Zamawiającego bez jego decyzji.

2.5. Funkcje monitorowania aktywności użytkowników (w szczególności z sekcji C i D tabeli w rozdz. 3) muszą być konfigurowalne niezależnie dla poszczególnych grup komputerów i użytkowników oraz możliwe do wyłączenia, w celu dostosowania zakresu monitorowania do regulaminu pracy i przepisów prawa pracy obowiązujących u Zamawiającego.

2.6. Wykonawca wskaże w ofercie minimalne wymagania sprzętowe i systemowe (procesor, pamięć RAM, przestrzeń dyskowa, system operacyjny, silnik bazy danych) niezbędne do działania każdej z instancji dla liczby stanowisk wskazanej w pkt 1.2.

2.7. Oprogramowanie musi być dostarczone w najnowszej wersji dostępnej na dzień dostawy. Interfejs użytkownika (konsola administracyjna, portal WWW, portal zgłoszeniowy i strona publiczna sygnalisty) musi być dostępny w języku polskim. Dokumentacja i pomoc kontekstowa muszą być dostępne w języku polskim (dopuszcza się wersję elektroniczną). Licencje i wsparcie muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej; Wykonawca przekaże dokumenty potwierdzające udzielenie licencji i rejestrację wsparcia na rzecz Zamawiającego.

2.8. Instancje dla sieci IT i OT muszą być od siebie całkowicie niezależne. Każda instancja musi działać samodzielnie, z własnym serwerem aplikacji, bazą danych, kontami użytkowników, konfiguracją i licencją, bez wspólnej konsoli zarządzania, synchronizacji danych lub konfiguracji ani połączeń sieciowych między instancjami.

3. Wymagania funkcjonalne Systemu

Oferowane oprogramowanie musi zapewniać co najmniej poniższe funkcjonalności, odrębnie w każdej z instancji (IT i OT), w zakresie sekcji wskazanych dla danej instancji w pkt 1.2.

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
A. Zarządzanie zasobami (sprzęt i wyposażenie)		
Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne		
1.	Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania	
2.	Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP, SNMP oraz WMI	
3.	Identyfikacja systemów Windows i Linux na podstawie skanu sieciowego	
4.	Automatyczne wykrywanie interfejsów sieciowych, ich typów oraz adresów IP, MAC, DNS, systemu operacyjnego wraz z informacją o aktualizacji	
5.	Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy	
6.	Odwzorowanie struktury organizacji w oparciu o Active Directory	
7.	Jednostronna synchronizacja komputerów oraz drukarek z AD, Entra ID oraz Intune (odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)	
8.	Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz Entra ID) oraz sieci	
9.	Mapowanie atrybutów obiektów AD (oraz Entra ID) do obiektów systemowych	
10.	Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)	
11.	Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)	
12.	Utworzenie własnych typów elementów wyposażenia	
13.	Łączenie elementów wyposażenia w zestawy	
14.	Przypisywanie zasobu do wielu zestawów	
15.	Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia	
16.	Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach	
17.	Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików	
18.	Przypisywanie sprzętu do konkretnych osób	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
19.	Przypisywanie sprzętu do wybranej firmy	
20.	Automatyczne wyznaczanie „głównego użytkownika” komputera	
21.	Wiązanie wielu rekordów wyposażenia z użytkownikiem	
22.	Przypisywanie sprzętu do dowolnej lokalizacji	
23.	Definiowanie własnych, dowolnych atrybutów sprzętu	
24.	Przydzielanie aktywnym komputerom (bez określonego statusu) statusu „W użyciu”	
25.	Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia	
26.	Dowolna treść kodu kreskowego	
27.	Określanie loga firmy oraz użycia go na wydrukach	
28.	Grupowa zmiana domeny/grupy roboczej zasobu	
29.	Możliwość łączenia zasobów w zestawy na podstawie typu oraz atrybutów zasobu	
Informacje o sprzęcie		
30.	Automatyczne wykrywanie typu komputera (Desktop/Notebook/Serwer/kontroler domeny) na podstawie wyników skanowania sprzętu	
31.	Wykrywanie komputerów typu All-In-One	
32.	Automatyczne wykrywanie typów stacji roboczej (Tower/Desktop/SFF/uSFF)	
33.	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	
34.	Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM	
35.	Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany	
36.	Definiowanie statusów dla sprzętu (nowy, do kasacji, w serwisie itd.)	
37.	Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)	
38.	Odczyt informacji o module TPM	
39.	Odczyt D3Dscore z WinSAT	
40.	Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: switch, router, access point, bridge, modem, NAS, UPS itd.)	
41.	Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu	
42.	Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika)	
43.	Automatyczne tworzenie zestawów: komputer + monitor	
44.	Automatyczne utworzenie zestawów: komputer + drukarka lokalna	
45.	Automatyczne utworzenie zestawów: host + maszyny wirtualne	
46.	Automatyczne wykrywanie czy komputer jest maszyną wirtualną	
47.	Wykrywanie maszyn wirtualnych typu Parallels Virtual Platform	
48.	Określanie informacji o wykorzystywanej wirtualizacji	
49.	Podgląd zestawów, do których należy zasób	
50.	Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami	
51.	Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu	
52.	Definiowanie szczegółowych informacji finansowych	
53.	Obsługa walut w danych finansowych	
54.	Definiowanie bazy dostawców sprzętu i oprogramowania	
55.	Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu)	
56.	Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta	
57.	Odczyt przez agenta identyfikator SID komputera	
58.	Określanie adresu interfejsu webowego urządzenia sieciowego	
59.	Określanie typu gwarancji dla zasobu	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
60.	Określenie wpływu biznesowego wybranego zasobu	
61.	Tworzenie własnych typów gwarancji	
62.	Określanie ikony dla typów zasobów	
63.	Integracja z API producenta sprzętu, co najmniej Dell	
64.	Wyszukiwanie i identyfikacja duplikatów zasobów	
65.	Geolokalizacja komputerów z agentem	
Raporty zasobów		
66.	Raport dodanych załączników	
67.	Automatyczne tworzenie historii zmian sprzętu	
68.	Raport zbiorczy historii zmian w sprzęcie	
69.	Ewidencja zdarzeń serwisowych	
70.	Dodawanie notatek/komentarzy dla zdefiniowanych obiektów zasobów	
71.	Informacja na temat pojemności dysków twardych oraz wolnego miejsca	
72.	Wydruk/dodawanie jako załącznik protokołu przekazania/zwrotu/utylizacji sprzętu	
73.	Wydruk/dodawanie jako załącznik protokołu przekazania dla całego zestawu	
74.	Kreator szablonów wydruków WYSIWYG	
75.	Definiowanie dedykowanych profili protokołów	
76.	Generowanie protokołów szyfrowania komputerów / telefonów	
77.	Zapisywanie protokołów podczas generowania jako załącznik do zasobu	
78.	Wydruk/dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia	
79.	Wydruk lub zapis do pliku raportów ze szczegółami sprzętu	
80.	Porównywarka wyników skanowania sprzętu	
81.	Dzienniki zdarzeń systemu Windows	
82.	Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu	
Zarządzanie zasilaniem		
83.	Zdalne włączanie i wyłączenie komputerów	
84.	Obsługa SecureOn przy Wake-on-LAN	
85.	Tworzenie harmonogramów wyłączania i włączania komputerów	
86.	Wybór trybu zamknięcia systemu, co najmniej: Blokada komputera, Uśpienie, Hibernacja, Wyłączenie, Wymuszenie wyłączenia, Restart	
87.	Możliwość anulowania /wyświetlenia komunikatu, jeśli jest zalogowany użytkownik	
88.	Możliwość przerwania / odłożenia zadania na żądanie użytkownika	
89.	Wymuszenie wylogowania użytkownika przed wyłączeniem komputera	
90.	Raport zadań jednorazowych oraz harmonogramów	
91.	Monitoring obciążenia CPU	
Funkcje dodatkowe		
92.	Zdalne wykonywanie skryptów (batch/PowerShell) – Obsługa zadań jednorazowych i cyklicznych	
93.	Generowanie skryptów z wykorzystaniem AI	
94.	Podpisywanie skryptów PowerShell certyfikatem	
95.	Wykonywanie skryptów w kontekście sesji użytkownika lub usługi	
96.	Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika	
97.	Wykonywanie zadań dla wszystkich komputerów	
98.	Edytor skryptów z funkcją kolorowania składni	
99.	Wykorzystywanie predefiniowanych skryptów	
100.	Import informacji o wyposażeniu z pliku CSV	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
101.	Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta sprzętu, co najmniej Dell	
102.	Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu)	
103.	Generowanie kodów kreskowych i QR dla każdego elementu wyposażenia	
104.	Obsługa kodów QR	
105.	Archiwum zasobów	
106.	Przeniesienie utylizowanego wyposażenia do archiwum	
107.	Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego	
108.	Powiadomienia o kończącej się gwarancji/umowie serwisowej dla zasobu	
109.	Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych	
110.	Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej	
111.	Grupowa zmiana atrybutów	
112.	Personalizacja statusów zasobów	
Magazyn		
113.	Kompleksowa obsługa gospodarki magazynowej	
114.	Kontrola stanów magazynowych	
115.	Rejestrowanie przyjęć i wydań towarów	
116.	Zarządzanie dokumentami magazynowymi	
117.	Monitorowanie przepływu zasobów pomiędzy lokalizacjami	
118.	Możliwość definicji typu towaru oraz określenia czy jest to zasób czy materiał eksploatacyjny	
119.	Generowanie dokumentów magazynowych: likwidacja, przesunięcie magazynowe (wydanie), przesunięcie magazynowe (przyjęcie), przyjęcie wewnętrzne, przyjęcie zewnętrzne, rozchód wewnętrzny, wydanie zewnętrzne	
120.	Dostosowanie szablonu dokumentów do własnych potrzeb	
121.	Definiowanie maski numeracji dokumentów magazynowych	
122.	Historia dokumentów magazynowych	
123.	Historia towarów magazynowych	
Aplikacja mobilna		
124.	Aplikacja mobilna Android do obsługi zasobów, transferów oraz skanowania RFID	
125.	Przekazywanie mienia (transfer zasobów) z obsługą weryfikacji i potwierdzania odbioru	
126.	Inwentaryzacja i identyfikacja zasobów z wykorzystaniem kodów RFID	
127.	Raportowanie sesji skanowania kodów RFID	
B. Zarządzanie oprogramowaniem		
Licencje		
128.	Inwentaryzacja licencji	
129.	Automatyczne tworzenie licencji na podstawie kluczy produktów	
130.	Odczyt klucza OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego	
131.	Import licencji z pliku tekstowego	
132.	Automatyczne generowanie historii zmian w licencji	
133.	Określanie statusu licencji	
134.	Tworzenie własnych atrybutów licencji	
135.	Tworzenie notatek oraz załączników w dowolnym formacie do licencji	
136.	Tworzenie licencji z poziomu rozliczenia audytu legalności	
137.	Tworzenie licencji z poziomu raportu kluczy licencji	
138.	Tworzenie zestawów licencji	
139.	Relacja licencji z użytkownikiem, firmą, działem, lokalizacją	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
140.	Zmiana typu licencji dla wybranej grupy	
141.	Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe)	
142.	Przypisywanie licencji do komputera	
143.	Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.)	
144.	Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska	
145.	Definiowanie licencji przeznaczonych do przyszłego zakupu	
146.	Definiowanie kluczy seryjnych i przypisywanie do licencji	
147.	Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją	
148.	Określenie wpływu biznesowego wybranej licencji	
Skanowanie oprogramowania		
149.	Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera	
150.	Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów	
151.	Śledzenie zmian w stanie zainstalowanego oprogramowania	
152.	Zdalny skan komputerów (bieżący lub okresowy)	
153.	Zmiana priorytetu skanowania oprogramowania	
154.	Skan komputerów niepodłączonych do sieci	
155.	Wysyłanie wyników skanowania offline na serwer FTP (Audyt)	
156.	Przekazywanie konfiguracji wzorcowej dla skanera offline	
157.	Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania	
158.	Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy	
159.	Określanie masek plików dla publikacji elektronicznych (e-book)	
160.	Skan plików skompresowanych	
161.	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	
162.	Odczyt skrótów MD5, SHA-1, SHA256, SHA384, SHA512 plików	
163.	Wbudowane profile skanowania (np. profil wzorcowy)	
164.	Definicja własnych ustawień skanowania	
165.	Porównywanie wyników skanowania oprogramowania	
166.	Wykrywanie plików multimedialnych	
167.	Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)	
168.	Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI	
169.	Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie	
170.	Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji/pakietów/systemów operacyjnych	
171.	Nadpisanie bazy wzorców najnowszą oficjalną bazą producenta	
172.	Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (* , %)	
Audyt oprogramowania		
173.	Rozliczanie pakietów aplikacji	
174.	Rozliczanie systemów operacyjnych	
175.	Rozliczanie licencji typu „downgrade”, „upgrade” oraz instalacji innego oprogramowania w ramach licencji	
176.	Audyt oprogramowania rozliczany automatycznie – informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji.	
177.	Historia audytów (wyniki audytów są przechowywane w bazie danych – można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)	
178.	Wsparcie procesu audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
179.	Gotowe metryki audytowanego komputera – załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)	
180.	Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji	
181.	Statystyki wykonanych audytów	
Funkcje		
182.	Mechanizm informujący o nowej bazie wzorców oprogramowania	
183.	Definiowanie własnych wzorców oprogramowania	
184.	Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych	
185.	Automatyczna klasyfikacja używanych programów z wykorzystaniem AI	
186.	Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania	
187.	Wykrywanie kluczy/identyfikatorów programów	
188.	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	
189.	Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office	
190.	Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania	
191.	Zbiorcze raporty wyników skanowania oprogramowania – Pakiety, pliki, systemy operacyjne, klucze zainstalowanych aplikacji	
192.	Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd.	
193.	Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.	
194.	„Wielkie raporty” (możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)	
195.	Zdalna instalacja oraz aktualizacja z katalogu oprogramowania Winget	
196.	Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi)	
197.	Zdalna dezinstalacja oprogramowania	
198.	Utworzenie harmonogramu dezinstalacji oprogramowania	
199.	Generowanie skryptu dezinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania	
200.	Raport stanu oprogramowania antywirusowego, antyszpiegowskiego oraz zapory sieciowej	
201.	Raport zainstalowanych aktualizacji systemu Windows	
C. Kontrola wykorzystania sprzętu i oprogramowania (monitoring użytkowników)		
Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne		
202.	Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) – jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach	
203.	Odczyt informacji o kontach lokalnych komputera, wraz z odczytem grup, do których konto należy	
204.	Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)	
205.	Określanie firmy, do której należy użytkownik	
206.	Określanie przełożonego dla użytkownika	
207.	Prezentacja „stanu użytkownika” (obecny, nieobecny, nowy)	
208.	Prezentacja 'statusu użytkownika' (zatrudniony, zwolniony itd.)	
209.	Zarządzanie stanowiskami użytkowników	
210.	Przeniesienie rekordu użytkownika do archiwum	
211.	Automatyczne generowanie historii zmian rekordu użytkownika (historia użytkownika)	
212.	Odczytywanie informacji o użytkownikach z Active Directory oraz Entra ID	
213.	Pełna synchronizacja rekordów użytkowników (odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz Entra ID)	
214.	Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
215.	Podgląd zdjęcia przypisanego do użytkownika	
216.	Przypisywanie do użytkownika załączników (pliki)	
217.	Przypisywanie notatek do użytkownika	
218.	Ewidencja zdarzeń przypisanych do użytkowników	
219.	Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory	
Raporty		
220.	Analiza aktywności użytkowników	
221.	Grupowanie danych według komputerów, jeśli użytkownik wykorzystywał więcej niż jedno stanowisko	
222.	Analiza zdarzeń sesji użytkownika (logowanie, wylogowanie, zablokowanie, odblokowanie, nawiązanie połączenia RDP, zakończenie połączenia RDP)	
223.	Analiza przerw w pracy	
224.	Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)	
225.	Analiza aktywności mikrofonu oraz kamery	
226.	Analiza wykorzystania poszczególnych aplikacji w czasie	
227.	Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie	
228.	Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika	
229.	Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny)	
230.	Statystyki najczęściej wykorzystywanych aplikacji	
231.	Statystyki wykorzystania komputerów przez poszczególnych użytkowników	
232.	Statystyki aktywności użytkownika i grup użytkowników	
233.	Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin	
234.	Kontrola wydruków – historia zadań drukowania zainicjowanych przez poszczególnych użytkowników	
235.	Kontrola wydruków – monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)	
236.	Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz.-b./kolor, dpi)	
237.	Monitoring wydruków na drukarkach sieciowych	
238.	Monitoring użytkowników stacji terminalowych	
239.	Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)	
240.	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	
241.	Raport zbiorczy historii zmian w rekordach użytkowników	
242.	Raport podsumowania aktywności użytkowników	
243.	Eksport danych czasu pracy z podziałem na czas pozytywny, neutralny i negatywny	
244.	Uwzględnienie dni tygodnia w raportach monitoringu użytkowników	
245.	Analiza odwiedzanych stron oraz kategorii odwiedzonych stron	
Funkcje		
246.	Blokada niepożądanych aplikacji – programy mogą być blokowane dla całej organizacji lub tylko dla wybranych użytkowników	
247.	Autoryzacja nośników zewnętrznych na podstawie wykrytych urządzeń	
248.	Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych	
249.	Automatycznie budowana baza informacji o napędach zewnętrznych	
250.	Automatyczna rejestracja wykrytych dysków zewnętrznych	
251.	Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)	
252.	Odczyt i blokada urządzeń PTP/MTP	
253.	Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM	
254.	Komunikacja z użytkownikami (komunikator, e-mail) bezpośrednio z zakładki Użytkownicy	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
255.	Informacje o ostatnio zalogowanych osobach na stacjach klienckich	
256.	Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje	
257.	Komentowanie przerw pracy	
258.	Akceptacja / odrzucenie przerwy w pracy na podstawie komentarza użytkownika	
259.	Akceptacja przerw pracy przez przełożonych	
260.	Automatyczne wykrywanie przerw w pracy (na podstawie aktywności użytkownika)	
D. Kontrola wykorzystania Internetu		
Funkcje		
261.	Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)	
262.	Blokada pobierania plików wg typu MIME	
263.	Blokada stron internetowych dla protokołu HTTP/HTTPS w najpopularniejszych przeglądarkach WWW	
264.	Kategoryzacja stron internetowych	
265.	Import stron WWW z pliku lub ze schowka	
266.	Słowniki kategorii stron WWW	
267.	Blokada dostępu do witryn zgodnie z harmonogramem	
268.	Blokada dostępu do witryn na podstawie kategorii strony WWW	
269.	Blokada trybu incognito w przeglądarce Google Chrome	
Raporty		
270.	Raporty dotyczące aktywności użytkowników w Internecie	
271.	Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki)	
272.	Monitoring stron internetowych dla protokołu HTTP/HTTPS (Przeglądarki oparte o silnik Chromium, Edge, Chrome, Vivaldi, Firefox)	
273.	Analiza liczby wejść na poszczególne strony lub domeny	
274.	Kategoryzacja odwiedzanych domen i stron, opcjonalnie z wykorzystaniem AI	
275.	Raport informujący o plikach pobranych przez przeglądarki WWW	
276.	Raport informujący o danych wysłanych przez przeglądarki (bez Firefox)	
277.	Monitoring plików pobieranych przez przeglądarki internetowe	
E. Helpdesk		
Obsługa zgłoszeń		
278.	Rejestracja i obsługa zgłoszeń	
279.	Obsługa zgłoszeń w modelu Kanban	
280.	Określanie relacji pomiędzy zgłoszeniami (np. kopia, incydent nadrzędny)	
281.	Edycja zgłoszeń powiązanych w oknie bieżącego zgłoszenia	
282.	Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii	
283.	Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów	
284.	Opis zgłoszenia w formacie HTML	
285.	Nawiązywanie połączeń zdalnych bezpośrednio z edytora zgłoszenia	
286.	Tworzenie notatek dla zgłoszeń	
287.	Zapisywanie wersji roboczej komentarza	
288.	Archiwizacja zgłoszeń	
289.	Monitoring czasu pracy nad incydentem (ang. time tracking)	
290.	Raport ewidencji czasu pracy nad zgłoszeniem	
291.	Informacja o czasie reakcji do podjęcia zgłoszenia	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
292.	Dodanie prywatnego komentarza	
293.	Znaki @ oraz # pozwalają na wspominanie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia	
294.	Dodanie załączników do incydentów, również do komentarza	
295.	Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie	
296.	Określanie uprawnień do incydentów (publiczne, prywatne, dla określonych działów)	
297.	Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń	
298.	Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń	
299.	Wydruk historii zgłoszenia	
300.	Widok kalendarza (planowanie rozwiązania incydentów)	
301.	Korelacja incydentu z elementem zasobów	
302.	Raport zbiorczy historii zmian	
303.	Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej	
304.	Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania	
305.	Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA	
306.	Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu	
307.	Określenie wpływu biznesowego wybranego zgłoszenia	
308.	Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń e-mail	
309.	Duplikacja i replikacja zgłoszeń	
310.	Powiadomienia o liczbie nieprzeczytanych zgłoszeń	
311.	Automatyzacja obsługi zgłoszeń z wykorzystaniem utworzonych reguł	
312.	Asystent AI do generowania odpowiedzi, podsumowania zgłoszenia, tłumaczeń, generowania tagów oraz wykrywania kategorii zgłoszeń	
313.	Obsługa formatu Markdown w asystencie AI	
314.	Podsumowania zgłoszeń generowane przez AI	
315.	Podsumowania komentarzy generowane przez AI	
Konfiguracja helpdesk		
316.	Architektura drzewa dla kategorii zgłoszeń	
317.	Tworzenie szablonów odpowiedzi	
318.	Cykliczne raportowanie listy incydentów	
319.	Tworzenie własnych dodatkowych atrybutów dla zgłoszeń	
320.	Tworzenie i zarządzanie typami statusów zgłoszeń	
321.	Personalizowane szablony wiadomości e-mail z możliwością ustawienia stałego załącznika	
322.	Notyfikacje e-mail o utworzeniu/zmianie/usunięciu incydentu	
323.	Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (Deadline)	
324.	Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP)	
325.	Weryfikacja rozmiaru załącznika wiadomości e-mail	
326.	Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox)	
327.	Możliwość filtrowania adresów e-mail w importerze wiadomości e-mail	
328.	Obsługa wielu kont pocztowych (import + notyfikacje e-mail)	
329.	Tworzenie własnych trybów oraz priorytetów incydentów	
330.	Personalizacja widoku raportu listy incydentów	
331.	Profile zgłaszających w helpdesk	
332.	Personalizacja kolorów statusów zgłoszeń	
333.	Automatyczne przypisywanie zgłoszeń do użytkowników	
334.	Weryfikacja wiadomości źródłowych pobieranych z serwera pocztowego	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
335.	Konfiguracja maksymalnej wielkości załącznika	
336.	Możliwość rejestrowania informacji o wyświetleniu zgłoszenia w historii	
Moduł połączeń zdalnych		
337.	Operacje na plikach i katalogach	
338.	Zarządzanie procesami i rejestrem	
339.	Monitoring pracy wykonywanej na komputerze	
340.	Zdalny podgląd pulpitów wielu stacji	
341.	Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji	
342.	Wysyłanie wiadomości do użytkowników	
343.	Uruchamianie na stacjach programów z wiersza poleceń	
344.	Zdalne uruchamianie komputera za pomocą funkcji Wake-on-LAN	
345.	Wake-on-LAN pozwala na definicję portu oraz adresu komputera docelowego	
346.	Przejęcie kontroli nad stacją roboczą	
347.	Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego	
348.	Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie	
349.	Przejęcie kontroli nad komputerem bez zalogowanego użytkownika	
350.	Wysyłanie pytania o zgodę na zdalny dostęp lub wysłanie komunikatu z informacją o rozpoczęciu podglądu pulpitu	
351.	Podgląd pulpitu zdalnego w osobnym oknie z opcją full-screen	
352.	Obsługa wielu monitorów dla podglądu pulpitu	
353.	Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu	
354.	Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie	
355.	Połączenie pulpitem zdalnym w konfiguracji NAT-NAT	
356.	Zarządzanie usługami systemu Windows	
357.	Raport sesji zdalnego pulpitu	
358.	Wybór adresu IP, na którym ma być zestawione połączenie zdalne	
359.	Wybór portu, na którym klient nasłuchuje połączenia zdalnego	
360.	Wykorzystanie własnego protokołu producenta lub MS RDP do połączeń zdalnych	
361.	Obsługa wiersza poleceń / PowerShell w trybie live	
362.	Raport sesji wiersza poleceń	
363.	Blokada kopiowania danych ze schowka operatora na komputer zdalny	
364.	Blokada połączeń w trybie informowania / cichym	
Baza wiedzy		
365.	Wbudowana baza wiedzy	
366.	Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk	
367.	Kopiowanie artykułów	
368.	Edytor HTML	
369.	Osadzanie załączników w treści artykułów	
370.	Osadzanie multimediów w treści artykułów	
371.	Baza wiedzy pozwala na tworzenie artykułów prywatnych oraz publicznych	
372.	Szybkie kopiowanie wpisów bazy wiedzy	
373.	Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk	
374.	Artykuły bazy wiedzy mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów	
375.	Informacja o liczbie odsłon artykułu bazy wiedzy	
376.	Bezpośrednie linkowanie artykułów bazy wiedzy	
SLA		

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
377.	Definiowanie planów umów SLA	
378.	Definiowanie czasu obowiązywania umów SLA	
379.	Definiowanie czasu pracy działów wsparcia technicznego	
380.	Definiowanie dni wolnych na podstawie kalendarza świąt i dni wolnych	
381.	Definiowanie czasów reakcji oraz realizacji zgłoszenia	
382.	Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji	
383.	Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie	
384.	Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną umową SLA	
F. Centralne repozytorium załączników		
Funkcje		
385.	Załączniki przechowywane w centralnym repozytorium	
386.	Utworzenie relacji załącznika z innymi elementami systemu 1–N (jeden do wielu)	
387.	Dodawanie i modyfikacja załączników z poziomu innych zasobów	
388.	Załączniki typu: link, udział oraz plik	
389.	Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura	
390.	Historia zmian załącznika	
G. Zarządzanie użytkownikami		
Funkcje		
391.	Raportowanie aktywności pracy	
392.	Przeglądanie ostatnio zgłoszonych incydentów	
393.	Powiązanie użytkownika z licencją	
394.	Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów	
395.	Cykliczne, automatyczne generowanie i dystrybucja mailowa raportów	
396.	Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze	
397.	Zgłoszenia dotyczące wniosków nieobecności użytkowników	
398.	Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności	
399.	Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika	
400.	Automatyczne utworzenie relacji przełożony – podwładny na podstawie skanów Active Directory	
401.	Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO	
402.	Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych	
403.	Planowanie dni wolnych w widoku kalendarza	
404.	Planowanie zastępstw podczas nieobecności	
405.	Blokowanie kont Windows	
H. Raportowanie cykliczne		
Raporty automatyczne, wysyłane e-mailem zgodnie z określonym harmonogramem oraz listą odbiorców:		
Użytkownicy		
406.	Raport historii sesji	
407.	Raport nośników danych	
408.	Raport operacji na plikach	
409.	Raport wydruków	
410.	Raport użycia aplikacji	
411.	Raport nagłówków okien [z możliwością wyłączenia]	
412.	Raport odwiedzonych stron WWW	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
413.	Raport najczęściej odwiedzanych stron internetowych	
414.	Raport wysyłanych plików	
415.	Raport czasu pracy przy komputerze	
416.	Raport agregujący statystyki użytkownika w rozbiciu godzinowym / kalendarzowym	
Zasoby		
417.	Raport historii zasobów	
418.	Raport informujący o nowych zasobach	
419.	Raport informujący o nadchodzących terminach w zasobach	
420.	Raport zasobów zarchiwizowanych	
421.	Raport systemów operacyjnych	
Podstawowe		
422.	Raport informacji o autoryzowanych agentach	
Oprogramowanie		
423.	Raport zainstalowanego oprogramowania	
424.	Raport szczegółów plików	
Helpdesk		
425.	Raport incydentów (Helpdesk)	
426.	Raport czasu pracy nad zgłoszeniem	
427.	Raport czasów SLA, obejmujący: czasy SLA, czas realizacji, historię zgłoszeń	
I. Automatyzacja		
Akcje (modyfikacje obiektów systemu, skrypty, powiadomienia mail / SMS / pop-up) wykonywane w przypadku wystąpienia wybranych wyzwalaczy.		
Wyzwalacze reguł – ogólne		
428.	Zakończenie okresu wsparcia producenta (asysty serwisowej)	
429.	Wygaśnięcie certyfikatu SSL	
430.	Kończące się licencje na agenta	
431.	Zapełniona baza danych	
432.	Dziennik operacji (uruchamiana po dodaniu wpisów do dziennika operacji)	
433.	Zbyt duży rozmiar folderu cache	
434.	Wygaśnięcie tokenu autoryzacyjnego API	
Wyzwalacze reguł – zasoby		
435.	Brak połączenia agenta	
436.	Brak wolnej przestrzeni na dysku	
437.	Ostrzeżenie od Windows Security Center	
438.	Zakończenie skanowania sprzętu	
439.	Powielenie agenta	
440.	Podłączenie dysku zewnętrznego	
441.	Stan modułu TPM	
442.	Stan szyfrowania woluminów	
443.	Dodanie zasobu	
444.	Zmiana zasobu	
445.	Usunięcie zasobu	
446.	Zakończenie okresu gwarancyjnego	
447.	Zakończenie umowy serwisowej	
448.	Powielenie zasobów	
449.	Nowy wpis w dzienniku zdarzeń Windows	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
Wyzwalacze reguł – oprogramowanie		
450.	Zmiana oprogramowania	
451.	Zakończenie skanowania oprogramowania	
452.	Zakończenie okresu wsparcia technicznego	
453.	Zamknięcie audytu	
Wyzwalacze reguł – licencje		
454.	Dodanie licencji	
455.	Zmiana licencji	
456.	Usunięcie licencji	
457.	Wygaśnięcie licencji	
458.	Planowana wymiana licencji	
Wyzwalacze reguł – użytkownicy		
459.	Dodanie użytkownika	
460.	Zmiana użytkownika	
461.	Usunięcie użytkownika	
462.	Logowanie użytkownika	
463.	Wylogowanie użytkownika	
464.	Strony WWW	
465.	Nagłówki okien	
Wyzwalacze reguł – helpdesk		
466.	Dodanie zgłoszenia	
467.	Usunięcie zgłoszenia	
468.	Zmiana zgłoszenia	
469.	Zapisana wersja robocza	
470.	Brak aktywności w zgłoszeniu	
Wyzwalacze reguł – RODO		
471.	Zbliżający się koniec dostępu	
Akcje reguł		
472.	Wykonywanie skryptu na podstawie zdefiniowanej reguły	
473.	Wysłanie powiadomienia w konsoli administracyjnej / portalu WWW na podstawie zdefiniowanej reguły	
474.	Wysyłanie powiadomienia mailowego na podstawie zdefiniowanej reguły (inicjator zdarzenia, administratorzy, konkretny użytkownik, rozwiązujący, zgłaszający, subskrybenci)	
475.	Modyfikacja zasobu / użytkownika / zgłoszenia – w zależności od reguły	
476.	Dodanie komentarza (dla reguł Helpdesk) [możliwe osobne reakcje na komentarz zgłaszającego / rozwiązującego]	
477.	Wysyłka wiadomości SMS	
478.	Wysyłka powiadomień do Microsoft Teams	
479.	Przypisanie atrybutu	
480.	Przypisanie / usunięcie reguł dostępu WWW	
481.	Podsumowanie zgłoszenia z wykorzystaniem AI	
482.	Uruchamianie reguł w harmonogramie	
J. RODO		
Funkcje		
483.	Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie	
484.	Filtrowanie zbiorów danych oraz czynności przetwarzania	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
485.	Wydruk raportów tabelarycznych: czynności przetwarzania, dostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie	
486.	Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia	
487.	Wstępne wypełnienie wniosków o zmianę dostępu	
488.	Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji	
489.	Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych	
490.	Archiwizacja zbiorów	
491.	Definiowanie czynności przetwarzania	
492.	Przypisywanie zbioru danych do czynności przetwarzania	
493.	Przydzielanie dostępów do czynności przetwarzania	
494.	Zapisywanie historii zmian wniosków o dostęp do zbiorów	
495.	Dodawanie historycznych dostępów oraz wniosków o dostęp	
496.	Filtrowanie użytkowników w raporcie „Dostępy”	
Raporty		
497.	Raport zbiorczy czynności przetwarzania	
498.	Raport zbiorczy zbiorów danych	
499.	Raport zbiorczy zinwentaryzowanych dostępów	
500.	Raport zbiorczy zinwentaryzowanych powierzeń	
501.	Raport zbiorczy zinwentaryzowanych dokumentów	
502.	Raport zbiorczy historii naruszeń bezpieczeństwa	
503.	Raport zbiorczy wniosków o dostęp	
504.	Raport zbiorczy dostępów	
K. Sygnalista		
Funkcje		
505.	Tworzenie zgłoszeń w postaci anonimowej lub nie anonimowej	
506.	Usuwanie metadanych z załączników zgłoszeń	
507.	Usuwanie danych osobowych ze zgłoszeń	
508.	Podział interfejsu na publiczny oraz wewnętrzny	
509.	Dashboard podsumowujący wykorzystanie portalu sygnalisty	
510.	Przypisywanie rozwiązujących zgłoszenia sygnalistów w zależności od typu zgłoszenia lub jego źródła	
511.	Definiowanie własnych atrybutów, kategorii, trybów zgłoszeń oraz poziomów ryzyka	
512.	Definiowanie stron publicznych (dostępnych dla sygnalistów)	
513.	Obsługa wielu języków stron publicznych	
514.	Natywne wsparcie języka ukraińskiego	
515.	Definiowany limit załączników	
516.	Wyróżnienie zgłoszeń o przekroczonym czasie reakcji	
517.	Blokowanie załączników do zgłoszeń	
518.	Pełna obsługa panelu sygnalisty za pomocą klawiatury	
519.	Integracja z zewnętrznym systemem wielosilnikowego skanowania plików (np. OPSWAT MetaDefender) w wersji instalowanej lokalnie oraz chmurowej	
520.	Skanowanie załączników programem antywirusowym	
521.	Własne opisy pól formularza sygnalisty	
522.	Obsługa zgód i akceptacji	
523.	Dostosowanie widoku sygnalisty do WCAG 2.2	
524.	Zabezpieczenie strony publicznej mechanizmem captcha	
Raporty		

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
525.	Raport zgłoszeń	
526.	Historia zmian	
527.	Statystyka zgłoszeń	
528.	Pozostały czas na przyjęcie zgłoszenia	
529.	Pozostały czas do zakończenia	
530.	Widgety: Kategorie zgłoszeń, Poziomy ryzyka, Tryby zgłoszeń, Statusy zgłoszeń, Ostatnio dodane	
L. Portal WWW		
Funkcje		
531.	Personalizacja portalu (logo, kolorystyka)	
532.	Wallboard – ekran zbiorczy prezentujący wybrane informacje z całego systemu	
533.	Personalizowany dashboard każdego modułu z najważniejszymi informacjami w postaci widgetów	
534.	Widok „Mój dzień” zawierający oś czasu z aktywnością użytkownika	
535.	Rozbudowane filtry dla raportów tabelarycznych	
536.	Zarządzanie użytkownikami, agentami, zasobami, licencjami, działami, audytami	
537.	Konfiguracja portalu helpdesk, kont administracyjnych oraz organizacji	
538.	Raporty dla każdego modułu w formie tabelarycznej	
539.	Obsługa helpdesk oraz bazy wiedzy	
540.	Obsługa modułu RODO	
541.	Obsługa modułu automatyzacja	
542.	Obsługa modułu Sygnalista	
543.	Automatyczne logowanie przy pomocy aplikacji	
544.	Logowanie za pomocą poświadczeń domenowych (SSO)	
545.	Logowanie za pomocą konta Microsoft Entra ID (dawniej Azure AD)	
546.	Wydruk raportów tabelarycznych	
547.	Kontrola statystyk użytkowników	
548.	Menu szybkiego dodawania nowych elementów (użytkownik, nieobecność, zasób, licencja, zgłoszenie, artykuł bazy wiedzy, zbiór danych, czynność przetwarzania)	
549.	Przełączanie wersji językowej bez ponownego logowania do systemu	
550.	Nawigacja typu breadcrumb	
551.	Definicja własnego URL, bez zmiany nazwy hosta (obsługa loadbalancingu)	
M. Powiadomienia push		
552.	Wysyłanie powiadomień wyświetlanych przez agenta na komputerach	
N. Funkcjonalności ogólne		
553.	Określanie praw dostępu do grup zasobów lub użytkowników	
554.	Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów (tzw. licencja pływająca)	
555.	Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem	
556.	Obsługa systemu w wielu zakładkach (również w aplikacji desktopowej)	
557.	Wersja angielska (en-US) interfejsu użytkownika	
558.	Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL	
559.	Swobodna migracja danych pomiędzy MS SQL i PostgreSQL	
560.	Zdalna instalacja i dezinstalacja agentów na stacjach roboczych	
561.	Odczytywanie struktury organizacji z Active Directory	
562.	Skaner sieci wykorzystywany do wykrywania nowych urządzeń	
563.	Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta	
564.	Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
565.	Automatycznie dodane komputery/użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory	
566.	Definiowanie nieograniczonej liczby użytkowników systemu	
567.	Role systemowe określane za pomocą uprawnień i kontroli dostępu	
568.	Role uprawnień – zestawy uprawnień pozwalające na szybkie ustawienie uprawnień użytkowników	
569.	Indywidualny login i hasło dla poszczególnych użytkowników	
570.	Automatyczne logowanie do systemu	
571.	Zarządzanie uprawnieniami użytkowników – określanie dostępu do poszczególnych obiektów i opcji systemu (konkretny użytkownik, konkretny zasób lub ich grupy), możliwość ograniczenia operacji (wyświetlanie, tworzenie, edycja, usuwanie)	
572.	Dostęp do programu chroniony przy pomocy uwierzytelniania wieloskładnikowego	
573.	Określanie ról użytkowników – zarządzanie grupami	
574.	Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem	
575.	Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)	
576.	Zgodność z pracą w sieciach WLAN	
577.	Podgląd aktualnych zadań serwera	
578.	Centrum informacji – przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników	
579.	Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami	
580.	Wyszukiwanie danych w tabelach raportów	
581.	Dowolne definiowanie grup sprzętu i użytkowników	
582.	Tworzenie dowolnych raportów ad-hoc – sortowanie kolumn, grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne	
583.	Definiowanie i zapamiętywanie własnych widoków	
584.	Eksport danych bezpośrednio do MS Excel	
585.	Budowa zestawień metodą drag'n'drop	
586.	Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów	
587.	Obsługa protokołu SSL/TLS zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server.	
588.	Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP	
589.	Mechanizm kompresji pakietów danych przesyłanych przez Agenta	
590.	Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery)	
591.	Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy)	
592.	Definiowanie konfiguracji serwera proxy dla połączenia Agent-Server	
593.	Mechanizm zdalnego pobierania bieżących aktualizacji do programu	
594.	Pomoc kontekstowa wraz z podręcznikiem użytkownika w polskiej wersji językowej	
595.	Dostęp do bazy wiedzy systemu	
596.	Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)	
597.	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	
598.	Manualna i automatyczna konserwacja bazy danych – usuwanie wyników skanowania oprogramowania, sprzętu, sesji zdalnego pulpitu, logów raportów, logów automatyzacji	
599.	Harmonogram konserwacji – planowanie godzin oczyszczania bazy	
600.	Personalizacja pakietu instalacyjnego agenta	
601.	Określanie polityki haseł dla systemu	
602.	Zmiana języka systemu podczas logowania	
603.	Określenie numeru BDO przy definiowaniu rekordu firmy	
604.	Opcja resetu hasła podczas logowania	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
605.	Globalne wyszukiwanie obiektów w systemie	
606.	Tworzenie atrybutów jako lista/słownik	
607.	Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników	
608.	Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring	
609.	Wyszukiwarka ustawień w opcjach systemowych	
610.	Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych)	
611.	Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie	
612.	Skanowanie lasu domen	
613.	Budowa personalizowanego pakietu instalacyjnego	
614.	Automatyczne zamknięcie konsoli administracyjnej po zakończeniu sesji	
615.	Logowanie do portalu Web za pomocą mechanizmu Single Sign On	
616.	Logowanie operacji kont serwisowych	
617.	Klucz bezpieczeństwa (Security Key) – dodatkowa metoda uwierzytelniania klientów przed połączeniem do serwera	
618.	Logowanie nieudanych prób uwierzytelnienia	
619.	Eksport danych diagnostycznych oraz dzienników operacji	
620.	Integracja z SMS API	
621.	Definiowanie nazwy hosta, na której serwer nasłuchuje połączeń sieciowych	
622.	Integracja z usługą modelu językowego (np. OpenAI) – asystent systemu	
623.	Osobisty token dostępu (PAT – Personal Access Token) do obsługi API	
O. API		
624.	API – moduł Firmy: pobieranie informacji o strukturze firm	
625.	API – moduł Lokalizacje: pobieranie listy lokalizacji	
626.	API – moduł Struktura organizacyjna: pobieranie widoku grup struktury organizacyjnej	
627.	API – moduł Użytkownicy: pobieranie danych użytkowników; aktualizacja użytkowników; pobieranie historii zmian użytkowników	
628.	API – moduł Zasoby: pobieranie informacji o zasobach; tworzenie zasobów; aktualizacja zasobów; pobieranie historii zmian zasobów; pobieranie statusów zasobów; pobieranie typów zasobów; pobieranie typów kodów kreskowych	
629.	API – moduł Załączniki: pobieranie załączników; tworzenie załączników plikowych; tworzenie załączników typu link	
630.	API – moduł Helpdesk: pobieranie zgłoszeń; tworzenie zgłoszeń; aktualizacja zgłoszeń; tworzenie komentarzy do zgłoszeń; pobieranie historii zmian zgłoszeń; pobieranie ewidencji czasu pracy nad zgłoszeniem; pobieranie kategorii, atrybutów, trybów, ważności, priorytetów i statusów zgłoszeń; pobieranie statusów dostępnych przy tworzeniu zgłoszenia; pobieranie ustawień rozwiązujących; pobieranie definicji umów SLA; pobieranie ustawień kont pocztowych	
P. Architektura i wymagania techniczne		
631.	Kreator instalacyjny ułatwiający wdrożenie systemu	
632.	Aplikacje konsoli administracyjnej (Master), serwera (Server) i agenta (Agent) w wersji x64	
633.	Aplikacja dla urządzeń mobilnych	
634.	Interfejs użytkownika dostępny w wielu językach, w tym w języku polskim	
635.	Rozproszona architektura systemu: serwer, konsola administracyjna, agent – z możliwością pracy każdego z komponentów na różnych komputerach	
636.	Praca w oparciu o MS SQL Server oraz MS SQL Express (2012 lub nowszy)	
637.	Praca w oparciu o PostgreSQL 11 lub nowszy	
638.	Szyfrowane połączenie pomiędzy serwerem aplikacji a bazą danych	
639.	Możliwość uruchomienia wielu równoległych instancji systemu	
640.	Obsługa systemów operacyjnych przez agenta: Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, Windows 7, 8, 10, 11	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
641.	Obsługa systemów operacyjnych przez konsolę administracyjną: Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, Windows 7, 8, 10, 11	
642.	Obsługa systemów operacyjnych przez serwer: Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, Windows 7, 8, 10, 11 oraz Linux	
643.	Wszystkie wykonywalne komponenty systemu podpisane certyfikatem Code Signing (Microsoft Authenticode) wydanym przez zaufany urząd certyfikacji	
644.	Sterowniki systemowe podpisane certyfikatem EV Code Signing (Extended Validation), umożliwiające pracę w 64-bitowych systemach operacyjnych Microsoft Windows	

W celu potwierdzenia zgodności oferowanego rozwiązania z wymaganiami Zamawiający żąda złożenia wraz z ofertą:

- wypełnionej tabeli załączonej do formularza ofertowego (zał. 2.1), ze wskazaniem producenta, nazwy i wersji oferowanego oprogramowania;
- dokumentacji producenta (np. specyfikacji funkcjonalnej, dokumentacji technicznej, opisu licencjonowania) potwierdzającej spełnienie wymagań z rozdz. 3, w tym bezterminowy charakter licencji oraz możliwość pracy i aktualizacji bez dostępu do Internetu (instancja OT).

Jeżeli z dokumentów producenta nie wynika jednoznacznie spełnienie danego wymagania, Wykonawca może złożyć oświadczenie producenta lub jego autoryzowanego przedstawiciela.

4. Wsparcie producenta

4.1. Wykonawca zapewni wsparcie producenta (asystę serwisową) dla obu instancji (IT i OT) przez okres 24 miesięcy, liczony od dnia podpisania protokołu odbioru licencji.

4.2. W ramach wsparcia Zamawiający otrzyma co najmniej: aktualizacje posiadanej wersji oprogramowania, prawo do aktualizacji do kolejnych wersji (upgrade), aktualizacje bazy wzorców oprogramowania, dostęp do bazy wiedzy i dokumentacji producenta oraz pomoc techniczną. Dla instancji OT producent musi udostępniać aktualizacje oprogramowania i bazy wzorców w postaci pakietów do instalacji w trybie offline.

4.3. Zgłoszenia przyjmowane są w dni robocze, przez portal producenta, e-mailem lub telefonicznie, w języku polskim. Czas reakcji na zgłoszenie: nie dłuższy niż **8** godzin roboczych.

5. Wdrożenie w sieciach IT i OT

5.2. Zasady wdrożenia w sieciach IT i OT

5.2.1. Wdrożenie obejmuje dwa niezależne środowiska: sieć IT oraz sieć OT Zamawiającego. W każdej z sieci Wykonawca wdroży odrębną instancję Systemu, zgodnie z pkt 2.8.

5.2.2. W trakcie prac Wykonawca nie może zestawiać połączeń między siecią IT a siecią OT, także tymczasowych, ani podłączać do sieci OT urządzeń lub nośników, które wcześniej były wykorzystywane w sieci IT, bez zgody Zamawiającego. Pakiety instalacyjne i aktualizacyjne dla instancji OT będą przenoszone w sposób uzgodniony z Zamawiającym, po weryfikacji ich integralności (suma kontrolna lub podpis producenta).

5.2.3. W sieci OT agent zostanie zainstalowany wyłącznie na komputerach z systemem Windows wskazanych przez Zamawiającego na piśmie (np. stacje operatorskie HMI, stacje inżynierskie, serwery systemów nadrzędnych), po potwierdzeniu przez Zamawiającego, że instalacja nie narusza warunków wsparcia ani certyfikacji systemu sterowania. Agent nie będzie instalowany na urządzeniach sterowania procesem (m.in. sterownikach PLC i RTU).

5.2.4. W instancji OT Wykonawca skonfiguruje System w sposób bezpieczny dla procesu technologicznego, w szczególności:

- aktywne skanowanie sieci (pkt 2 tabeli) zostanie ograniczone do zakresów adresowych wskazanych przez Zamawiającego, z wyłączeniem segmentów z urządzeniami sterowania procesem, i będzie uruchamiane wyłącznie w uzgodnionych oknach serwisowych;

- funkcje mogące wpływać na pracę stacji – zarządzanie zasilaniem (pkt 83–91 tabeli), zdalne wykonywanie skryptów, zdalna instalacja i dezinstalacja oprogramowania, blokada aplikacji oraz przejęcie kontroli nad stacją – zostaną wyłączone albo udostępnione wyłącznie wskazanym administratorom, z obowiązkiem ręcznego uruchomienia;
- funkcje monitorowania aktywności użytkowników (sekcje C i D, pkt 202–260 i 261–277 tabeli) zostaną skonfigurowane w zakresie wskazanym przez Zamawiającego;
- zostanie włączona kontrola nośników zewnętrznych i urządzeń PTP/MTP (pkt 247–253 tabeli), z listą nośników autoryzowanych uzgodnioną z Zamawiającym;
- funkcje wymagające dostępu do Internetu lub usług chmurowych (pkt 2.4) zostaną wyłączone.

5.2.5. Prace w sieci OT Wykonawca będzie prowadził wyłącznie w oknach serwisowych uzgodnionych z Zamawiającym, zgodnie z obowiązującymi u Zamawiającego procedurami bezpieczeństwa, w sposób niepowodujący przerw ani zakłóceń w procesie technologicznym. Instalacja agenta w sieci OT zostanie poprzedzona instalacją pilotażową na stacji wskazanej przez Zamawiającego.

5.3. Zakres wdrożenia (odrębnie dla sieci IT i dla sieci OT)

5.3.1. Przeprowadzenie analizy przedwdrożeniowej oraz opracowanie odrębnego projektu technicznego wdrożenia dla sieci IT i dla sieci OT, zawierającego architekturę, wymagania dla serwerów i bazy danych, zakres modułów i funkcji, polityki agentów, uprawnienia oraz harmonogram prac, przedkładanego do akceptacji Zamawiającego. Prace instalacyjne mogą rozpocząć się po akceptacji projektu.

5.3.2. Instalacja i konfiguracja serwera aplikacji, bazy danych, konsoli administracyjnej i portalu WWW w każdej z instancji, w tym szyfrowanie komunikacji (TLS), konfiguracja kont i ról, uwierzytelniania wieloskładnikowego i polityki haseł, kopii zapasowych bazy danych oraz utwardzenie konfiguracji (zmiana domyślnych haseł, wyłączenie zbędnych usług).

5.3.3. Integracja instancji IT z usługami katalogowymi Zamawiającego (Active Directory, Microsoft Entra ID / Intune), serwerem poczty i skrzynkami helpdesk **jeśli dotyczy**. Instancja OT zostanie zintegrowana wyłącznie z usługami działającymi w sieci OT.

5.3.4. Dystrybucja agentów na stanowiska wskazane przez Zamawiającego (w sieci IT – co najmniej **20** stanowisk, w sieci OT – stanowiska wskazane zgodnie z pkt 5.2.3), wykonanie inwentaryzacji sprzętu i oprogramowania oraz weryfikacja poprawności danych.

5.3.5. Konfiguracja modułów zgodnie z projektem, w tym: struktury organizacyjnej i lokalizacji, typów i statusów zasobów, licencji oraz pierwszego audytu legalności oprogramowania, kategorii zgłoszeń i umów SLA, reguł automatyzacji i powiadomień, a w instancji IT – modułu RODO i Sygnalista (w tym strony publicznej sygnalisty).

5.3.6. Przeprowadzenie testów odbiorczych w każdej z sieci, według scenariuszy przedłożonych Zamawiającemu do akceptacji, obejmujących co najmniej:

- inwentaryzację sprzętu i oprogramowania na stanowiskach testowych oraz wykonanie audytu legalności oprogramowania;
- w sieci IT – utworzenie zgłoszenia helpdesk z wiadomości e-mail i z portalu, naliczenie czasów SLA oraz przyjęcie zgłoszenia testowego w portalu sygnalisty;
- blokadę nieautoryzowanego nośnika zewnętrznego i dostęp do nośnika autoryzowanego;
- wyzwolenie reguły automatyzacji (np. brak połączenia agenta) i dostarczenie powiadomienia;
- aktualizację instancji OT w trybie offline;
- brak dostępu do interfejsów zarządzania spoza wyznaczonego segmentu zarządzania oraz brak połączeń między instancjami IT i OT.

5.3.7. Przekazanie odrębnej dla sieci IT i dla sieci OT dokumentacji powykonawczej w języku polskim, obejmującej co najmniej: opis architektury i konfiguracji, wykaz serwerów, kont technicznych i ról, opis polityk agentów i reguł automatyzacji, protokoły z testów oraz procedury administracyjne (instalacja agenta, aktualizacja – dla sieci OT również w trybie offline, kopia zapasowa i odtworzenie bazy danych). Hasła zostaną przekazane w sposób uzgodniony z Zamawiającym, odrębnie od dokumentacji.

5.3.8. Przeprowadzenie w siedzibie Zamawiającego instruktażu dla administratorów w wymiarze nie mniejszym niż **8** godzin dla maksymalnie **2** osób, obejmującego obsługę obu instancji oraz procedury z pkt 5.3.7.

5.3.9. Osoby realizujące wdrożenie po stronie Wykonawcy przed przystąpieniem do prac podpiszą zobowiązanie do zachowania poufności informacji uzyskanych w trakcie realizacji zamówienia, w szczególności dotyczących architektury i zabezpieczeń sieci IT i OT oraz danych osobowych przetwarzanych w Systemie. W zakresie, w jakim Wykonawca uzyska dostęp do danych osobowych, strony zawrą umowę powierzenia przetwarzania danych osobowych.

5.3.10. Wykonawca udzieli gwarancji na prawidłowe działanie wykonanej konfiguracji na okres nie krótszy niż **24** miesięcy od dnia odbioru wdrożenia w danej sieci.

6. Terminy realizacji i odbiór

6.1. Termin dostawy licencji i aktywacji wsparcia producenta: do 2**0** dni od dnia zawarcia umowy.

6.2. Termin realizacji wdrożenia: do **14** dni.

6.3. Odbiór licencji nastąpi na podstawie protokołu odbioru, po przekazaniu dokumentów licencyjnych dla obu instancji oraz potwierdzenia rejestracji wsparcia producenta.

6.4. Odbiór wdrożenia nastąpi odrębnie dla sieci IT i dla sieci OT, na podstawie protokołów odbioru podpisanych po pozytywnym wyniku testów z pkt 5.3.6 oraz przekazaniu dokumentacji z pkt 5.3.7. Po odbiorze wdrożenia w obu sieciach i przeprowadzeniu instruktażu strony podpiszą protokół odbioru końcowego.

7. Rozwiązania równoważne

7.1. Wskazanie w OPZ nazw systemów, usług i technologii, z którymi oferowane oprogramowanie musi współpracować (m.in. Microsoft Windows, Active Directory, Microsoft Entra ID, Intune, Microsoft Teams, MS SQL Server, PostgreSQL, Winget, Dell), wynika z infrastruktury wykorzystywanej przez Zamawiającego i nie stanowi wskazania oferowanego produktu.

7.2. Pozostałe nazwy własne, znaki towarowe lub normy wskazane w OPZ mają charakter przykładowy. Zamawiający dopuszcza rozwiązania równoważne, zgodnie z art. 99 ust. 5 i art. 101 ust. 4 ustawy Prawo zamówień publicznych. Wykonawca, który powołuje się na rozwiązanie równoważne, jest obowiązany wykazać, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego.