Załącznik nr 1 do zapytania ofertowego

Opis przedmiotu zamówienia

CZĘŚĆ 1

Zakup oprogramowania do zintegrowanego zarządzania bezpieczeństwem infrastruktury informatycznej Urzędu, MGOPS i GZK.

Przedmiot zamówienia dla części 2 obejmuje zakup oprogramowania do zintegrowanego zarządzania bezpieczeństwem infrastruktury informatycznej urzędu – 1 licencji wieczystej z 80 agentami i jednostek urzędu: Miejsko-Gminnego Ośrodka Pomocy Społecznej w Sianowie (MGOPS) – 1 licencji wieczystej z 60 agentami oraz Gminnego Zakładu Komunalnego w Sianowie (GZK) – 1 licencji wieczystej z 30 agentami.

Na potrzeby urzędu - 1 licencji wieczystej z 80 agentami i dwóch większych jednostek podległych: MGOPS – 1 licencji wieczystej z 60 agentami, GZK – 1 licencji wieczystej z 30 agentami zostanie zakupione oprogramowanie ze wsparciem technicznym przez okres 12 miesięcy, które umożliwi zintegrowane zarządzanie i bezpieczeństwo IT lokalnych sieci komputerowych. Oprogramowanie będzie zawierać następujące funkcjonalności:

- monitorowanie urządzeń sieciowych: monitorowanie urządzeń pojawiających się i działających w sieci LAN, informacje o potencjalnych awariach w sieci,
- ochrona danych i zarządzanie zabezpieczeniami: zwiększenie poziomu bezpieczeństwa w organizacji poprzez ochronę danych i zarządzać zewnętrznymi zabezpieczeniami z poziomu jednej konsoli,
- system zgłoszeń i zdalne wsparcie: zarządzanie zgłoszeniami pracowników i odpowiadanie na nie w łatwy sposób oraz udzielanie im zdalnej pomocy,
- zarządzanie czasem i mierzenie aktywności pracowników: zidentyfikowanie aktywności pracowników i zespołów, które pochłaniają najwięcej czasu, zoptymalizowanie efektywności pracy w kluczowych obszarach,
- bezpieczeństwo danych i zarządzanie użytkownikami: zapobieganie problemom z bezpieczeństwem firmowych danych oraz sprawne zarządzanie dostępami i uprawnieniami użytkowników,
- zarządzanie zasobami IT: lista zainstalowanego oprogramowania, rozliczanie licencji, inwentaryzacja sprzętu oraz zarządzanie wszystkimi zasobami IT w jednym miejscu.

Specyfikacja oprogramowania:

Oprogramowanie powinno posiadać budowę modułową, składającego się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Instalacje zdalnych konsoli zarządzania nie powinny podlegać limitom i nie powinny być objęte dodatkowym licencjonowaniem. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2. Program powinien umożliwić zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.

Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy, bezpieczny, stabilny i wysoce wydajny silnik bazy danych z kodem źródłowym dostępnym na licencji open-source, dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Agent programu powinien korzystać z bazy danych z wydajnym i stabilnym silnikiem, która nie wymaga dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających może być przeprowadzona na 64-bitowym systemie operacyjnym Windows w tym m.in. Windows Serwer 2022 w wersji Standard. Oprogramowanie powinno zawierać rozbudowany system raportowy zawierający raporty predefiniowane oraz umożliwiający tworzenie własnych raportów wraz z możliwością pełnego dostosowania wyglądu.

Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Powinny być one również grupowane w osobnym, dedykowanym oknie. Pozwali 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, powinny być objęte kontrolą na poziomie wybranych Administratorów – w programie można będzie nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator będzie miał 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. Działania administratorów powinny być logowane oznacza to, że program powinien posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog. Lista kont użytkowników, w tym administratorów, może być synchronizowana z Active Directory wraz z awatarami, również przez szyfrowane połączenie LDAPS. Program powinien umożliwiać również tworzenie lokalnych kont użytkowników wraz z awatarami w środowiskach bez Active Directory. Liczba kont użytkowników w konsoli nie powinna być objęta limitem i nie podlegać licencjonowaniu.
Program powinien umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityka ta powinna pozawalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad. Program powinien zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS.
W weryfikacji MFA będzie można skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera.

MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) powinno obejmować 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 kolorem tła.
-wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła 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 powinien monitorować czas ich odpowiedzi i procent utraconych pakietów
-serwerów pocztowych:
- program powinien monitorować czas logowania do serwisu odbierającego oraz czas wysyłania poczty
- program powinien mieć 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
- monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
- zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
-wydajności systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

Program powinien 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). 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 kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.

Program powinien umożliwiać 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, wysłanie wiadomości SMS poprzez integrację z serwisem sms, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie /restart sługi Windows, wyłączenie/restart komputera. Alarmy powinny być 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. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. Nie wykonuj między 9:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności I typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji.

Program powinien mieć możliwość integracji ze sprzętową bramką GSMHW-SMS-GW3 w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP) oraz poprzez integrację z bramkami SMS.

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

1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Umożliwiać odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.

3. Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
4. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
5. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
6. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
7. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
8. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
10. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
11. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji powinny być logowane.
Moduł inwentaryzacji zasobów powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:
-przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
-przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
-tworzenia powiązań między zasobami a urządzeniami,
-tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
-tworzenia relacji pomiędzy zasobami,
-wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
-definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości
-dla danego urządzenia lub oprogramowania powinna istnieć 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,
- masową edycję atrybutów 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,
- możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- 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").

Oprogramowania powinno zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
1) skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP,
2) informacje o aplikacjach używanych w organizacji,
3) tworzenie własnych wzorców aplikacji,
4) tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.,
5) informacje o komputerach, na których aplikacja została wykryta,
6) zarządzanie posiadanymi licencjami,
7) wskazywanie osób odpowiedzialnych za licencję,
8) wskazanie użytkowników licencji,
9) tworzenie powiązań między licencjami a dokumentami w relacji 1:N,
10) 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,
11) łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych,
12) zarządzanie posiadanymi licencjami: raport zgodności licencji,
13) możliwość przypisania do programów numerów seryjnych, wartości itp.
Okna audytowe posiadają możliwość filtrowania elementów per oddział.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program powinien 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 (tytuły, adresy, liczba i czas 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. Program ma możliwość monitorowania kosztów wydruków,
- nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.
Program ponadto powinien posiadać możliwość:
- wykrywania podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy,
- zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury,
- wyszczególnienia podejrzanej aktywności w raportach,
- wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności,
- automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności,
- 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 lub współdzielone pomiędzy grupami lub kontami,
- integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT,
- skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia,
- automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych,
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- prowadzenia rejestru naruszeń blokad,
- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych wciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
- 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 ActiveDirectory 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 powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz zblokowania aplikacji i stron internetowych.
Program powinien umożliwiać realizację zdalnej pomocy użytkownikom.
W ramach kontroli stacji użytkownika dostępny powinien być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.
W module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwalać powinno na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł powinien umożliwiać również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością powinno być

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. System powinien umożliwiać użycie pośredniego statusu „zgłoszenie rozwiązane" przed ostatecznym zamknięciem zgłoszenia.
Moduł ten powinien zawierać 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 powinien pozwalać na:
- zarządzanie dostępem do czatu w min. 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy techniczne,
- rozmowy również między „zwykłymi" użytkownikami,
- osadzanie załączników w treści wiadomości,
- osadzanie obrazków w treści wiadomości,
- formatowanie tekstu,
- tworzenie pokojów tematycznych, rozmów grupowych,
- oznaczanie kontaktów jako „ulubionych" na liście kontaktów,
- uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku,
- może być wyświetlany w trybie jasnym lub ciemnym.

W module powinna być zawarta baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program powinien umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik powinien mieć możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.
Dostęp do systemu zgłoszeń oraz bazy wiedzy powinien być realizowany przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.
Moduł pomocy zdalnej powinien umożliwiać również:
- pobieranie listy użytkowników z Active Directory wraz z awatarami,
- wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
- zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
- zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
- zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
- zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
- 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,
- definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
- przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
- procesowanie zgłoszeń użytkowników z wiadomości e-mail,
- dostęp do plików źródłowych wiadomości e-mail przetworzonych na zgłoszenia,
- obsługę wielu adresów e-mail jednego użytkownika w celu przetwarzania jako zgłoszeń pochodzących od tej samej osoby,
- eksportowania listy zgłoszeń do plików CSV i XLSX,
- integrację ze wieloma skrzynkami e-mail w celu obsługi różnych kanałów zgłoszeń wraz z automatyzacjami,
- integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,

- tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
- wykonywanie operacji na wielu zgłoszeniach równocześnie,
- dołączanie załączników do zgłoszeń,
- usuwanie zamkniętych 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 w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
- zrzuty ekranowe (podgląd pulpitu),
- zdalną modyfikację rejestrów, swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika,
- dystrybucję oprogramowania przez Agenta,
- definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
- przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
- dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
- zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
- możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
- możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
- 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 Agenta (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 bez blokowania interfejsu programu podczas przesyłania plików.

MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych. Program powinien mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.

10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:
1) definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików,
2) autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp.,
- 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,
3) monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika,
4) definiowanie reguł monitorowanych folderów w postaci list,
5) monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.),
6) integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych,
7. przydzielanie uprawnień również do kont użytkowników lokalnych. Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.

Dodatkowe wymagania:
W ramach oferty Zamawiający otrzymuje:
- licencję wieczystą na oprogramowanie,
- moduł sieciowy dla nielimitowanej liczby monitorowanych urządzeń,
- instalację wielu zdalnych konsol administracyjnych,
- 12 miesięcy umowy serwisowej (aktualizacje i pomoc techniczną),
- możliwość przedłużenia umowy serwisowej na kolejne 12 miesięcy (przy zachowaniu ciągłości usługi) z rabatem 80% względem ceny aktualnej, nowej licencji,
- możliwość dokupienia modułów (rozszerzenia funkcjonalności) oraz zwiększenia liczby zarządzanych stacji roboczych w ramach jednej licencji w dowolnym czasie,
- zdalne wdrożenia (w trzech lokalizacjach: urząd, GZK i MGOPS) oraz przeszkolenie trzech administratorów (w trzech lokalizacjach: urząd, GZK i MGOPS) z podstawowych zasad konfiguracji i pracy na oprogramowaniu do zintegrowanego zarządzania bezpieczeństwem infrastruktury informatycznej w tym m.in.:
1) instalacja przez Usługodawcę (najnowszej wersji oprogramowania) na udostępnionej przez Zamawiającego (w trzech lokalizacjach: urząd, GZK i MGOPS) wirtualce Hyper-V z Windows Serwerem Standard 2022
2) konfiguracja i kontrola profili pracy agenta,
3) konfiguracja i kontrola zakresu przechowywania danych w bazie Oprogramowania (retencja danych),
4) konfiguracja i kontrola pracy modułu sieciowego,
5) konfiguracja i kontrola obciążenia krytycznych urządzeń (CPU, RAM, HDD, i inne),
6) monitorowanie pracy najważniejszych urządzeń, serwisów i usług,
7) alarmy i raporty,
8) kontrola i konfiguracja pracy modułu inwentaryzacyjnego,
9) profile pracy agenta „per Urządzenie",
10) pliki na PC,
11) raporty i Alarmy,

12) kontrola i konfiguracja pracy modułu użytkowników,
13) grupy monitorowanych aplikacji,
14) grupy monitorowanych stron,
15) grupy użytkowników (lokalne i AD),
16) profile pracy agenta „per User”,
17) ograniczenie „per User” analiza i komunikaty blokady,
18) alarmy „per User”,
19) konfiguracja i kontrola pracy modułu Pomocy,
20) analiza kategorii zgłoszeń,
21) powiadamianie i workflow zgłoszeń,
22) raporty,
23) kontrola i konfiguracja pracy modułu Ochrony Danych,
24) grupy użytkowników (lokalne i AD),
25) profile pracy Ochrony Danych „per User”,
26) alarmy i raporty,
27) dobre praktyki i propozycje scenariusza pracy z oprogramowaniem.

Wszystkie powyższe usługi (termin i zakres) powinny być wykonane w uzgodnieniu z obsługą informatyczną urzędu i jednostek.

CZĘŚĆ *2* :
Zakup dostępu do platformy szkoleniowej z cyberbezpieczeństwa dla Urzędu, MGOPS i GZK.

Przedmiot zamówienia dla części 2 obejmuje zakup platformy szkoleniowej z cyberbezpieczeństwa dla urzędu - 60 dostępów i jednostek urzędu: Miejsko-Gminnego Ośrodka Pomocy Społecznej w Sianowie (MGOPS) – 40 dostępów oraz Gminnego Zakładu Komunalnego w Sianowie (GZK) – 30 dostępów.

Platforma szkoleniowa bezpieczeństwa dostarczy wiedzę, dobre praktyki i możliwość testowania użytkowników w celu ochrony cennych zasobów urzędu i jednostek podległych. Szkolenia pozwolą pracownikom nabywać niezbędne umiejętności do bezpiecznego poruszania się w cyfrowym świecie. Pozwoli na regularną, konsekwentną naukę na zróżnicowanym poziomie – bez problemów związanych z absencją
w dniu szkolenia lub niedostateczną koncentracją. Pracownicy zyskują możliwość oceniania zaangażowania i poziomu wiedzy. Obsługa informatyczne będzie mogła łatwo zidentyfikować luki w wiedzy i złe nawyki, a w następstwie szybko wdrożyć procedury naprawcze. W temacie szkoleń znajdą się m.in. takie tematy: Socjotechniki, bezpieczeństwo haseł, bezpieczeństwo poczty, ochrona przed phishingiem, bezpieczeństwo stron www i przeglądarek, dobre praktyki bezpieczeństwa i inne.
Specyfikacja usługi:
Kompleksowa platforma *powinna* dostarczyć narzędzia i zasoby niezbędne do zapewnienia pracownikom wartościowej wiedzy i umiejętności w zakresie ochrony przed cyberzagrożeniami. Użytkownicy powinni otrzymać dostęp do materiałów szkoleniowych oraz testów wiedzy. Menedżerowie grup oraz administratorzy powinni zyskać wgląd w postęp nauki i poziom wiedzy w całej organizacji i dla poszczególnych grup.

Platforma powinna zawierać m.in.: dedykowane kursy o bezpiecznej pracy w Internecie, ochronie danych osobowych podzielone na moduły, lekcje i testy.
Ponadto powinna mieć: statystyki i raporty dla użytkowników, grup i menadżerów, możliwość dodawania własnych materiałów

Platforma powinna być stale rozwijana pod kątem funkcjonalnym jak i zwiększaniem zawartości szkoleniowej.

Architektura Platformy:
Platforma powinna pracować w systemie chmurowym, który nie wymaga konserwacji przez nabywcę.

Cechy organizacji:
Po zakupie subskrypcji, Usługobiorca powinien otrzymać wyłączny dostęp do nowo utworzonej organizacji. Nazwa organizacji będzie definiowana w trakcie procesu zakupowego. Razem z organizacją utworzone zostanie konto Administratora Głównego. Administratorem danych konta Administratora Głównego jest Producent (**Usługodawca).** Wraz z nazwą organizacji konfigurowana jest nazwa domeny organizacji.
W każdej organizacji powinno być jedno konto Administratora Głównego. Administrator Główny powinien dodawać lub importować konta pierwszych użytkowników do platformy. Administratorem danych użytkowników Organizacji powinien być Usługobiorca subskrypcji – Administrator Główny.
Administrator Główny może powierzyć zadanie zarządzania organizacją innym użytkownikom poprzez nadanie im roli Administratora.
Każda organizacja powinna mieć możliwość utworzenia m.in. 1000 użytkowników oraz 500 grup.

Część szkoleniowa
Platforma powinna udostępniać swoim użytkownikom m.in. dwa kursy: pierwszy, z zakresu cyberbezpieczeństwa "Bezpieczna praca w Internecie", który składa się z modułów, lekcji i testów sprawdzających nabytą przez kursantów wiedzę oraz drugi, omawiający zagadnienia bezpieczeństwa i przetwarzania danych osobowych zgodnie z RODO – „Wprowadzenie do RODO", który składa się z modułów, lekcji i testów sprawdzających wiedzę.
Każdy moduł składa się z lekcji w formie video oraz testu. Oprócz testów wewnątrz modułu, kurs zawiera również testy obejmujące swoim zakresem tematycznym przekrojowo więcej niż 1 moduł szkoleniowy.
Szkolenia powinny być przygotowane i odpowiednio ułożone przez ekspertów w dziedzinie cyberbezpieczeństwa oraz ochrony danych osobowych, a informacje w nim zawarte aktualne istotne i odnoszące się do realnych zagrożeń, na które użytkownik może natknąć się podczas codziennego korzystania z komputera w pracy i nie tylko.
Minimalny zakres tematyczny kursu „Bezpieczna praca w Internecie":
- socjotechniki,
- bezpieczeństwo haseł,
- bezpieczeństwo poczty e-mail i ochrona przed SCAM-em,
- obrona przed phishingiem,
- bezpieczeństwo stron WWW i przeglądarek,
- ataki socjotechniczne z wykorzystaniem urządzeń,
- ataki za pośrednictwem telefonu,
- zagrożenia związane w urządzeniami mobilnymi,
- zagrożenia związane z sieciami Wi-Fi,
- zagrożenia w mediach społecznościowych,
- dobre praktyki bezpieczeństwa,
- prywatność, poufność i anonimowość w Internecie.

Minimalny zakres tematyczny kursu „Wprowadzenie do RODO":
- RODO – wstęp dla każdego pracownika,
- incydenty i naruszenia ochrony danych,
- RODO – w przykładach i praktyce stosowania,
- Powierzenie przetwarzania danych i wybór dostawcy.

Cechy szkolenia:

- umożliwia szczegółowe monitorowanie postępu użytkownika,
- statusy lekcji: nierozpoczęta, w toku, ukończona,
- statusy modułu: nierozpoczęty, w toku, ukończony,
- statusy testu: nierozpoczęty, rozpoczęty, niezaliczony, zaliczony,
- brak ustalonej kolejności kursu, użytkownik może od razu przejść do zaliczenia testu lub zapoznawać się z lekcjami video według uznania lub według narzuconego w organizacji harmonogramu.
- każdy moduł powinien zawierać krótkie streszczenie zawartości,
- każda lekcja powinna zawierć notatki w formie tekstowej,
- po ukończeniu materiału użytkownik wciąż ma do niego nieograniczony dostęp w ramach trwającej subskrypcji, przypisanej do organizacji,
- postęp w lekcji jest zapisywany, użytkownik po powrocie do danej lekcji zaczyna od momentu, w którym zakończył oglądanie materiału video,
- kurs umożliwia filtrowanie dostępnych modułów kursu (wszystkie moduły, nowe, rozpoczęte, ukończone),
- kurs pozwala użytkownikowi na ukrywanie ukończonych lekcji,
- po ukończeniu każdego modułu kursu użytkownik otrzymuje certyfikat (do wydruku),
- po ukończeniu kursu użytkownik otrzymuje certyfikat (do wydruku),
- administrator platformy ma możliwość konfigurowania minimalnego postępu w kursie (tempa postępów) osiąganego przez użytkowników,
- szkolenie dostępne również w wersji mobilnej z poziomu przeglądarki, bez konieczności instalacji dodatkowego oprogramowania.

Test:
- składać się powinien z pytań i odpowiedzi jednokrotnego wyboru,
- do testu będzie można podejść przed ukończeniem lekcji video (dowolna kolejność wykonywania działań w obrębie kursu),
- administrator platformy powinien mieć możliwość konfigurowania progu punktowego wymaganego do zaliczenia testu,
- administrator platformy powinien mieć możliwość konfigurowania czasu, który musi upłynąć zanim użytkownik po raz kolejny może podejść do testu,
- test zapamiętuje odpowiedzi użytkownika (na wypadek opuszczenia testu przed ukończeniem),
- kolejność pytań i odpowiedzi jest losowana przed rozpoczęciem przez użytkownika testu,
- ukończenie/Zaliczenie testu wpływa na postęp ukończenia modułu,
- brak limitu czasowego na ukończenie testu,
- zmiana wymaganego w organizacji progu procentowego zaliczenia testu po ukończeniu przez użytkownika testu nie ma wpływu na status testu (zaliczony/niezaliczony),
- kursy zawierają test końcowy sprawdzający wiedzę z całego kursu.

ZARZĄDZANIE PLATFORMĄ
Zarządzanie użytkownikami:
- podział na 3 role: właściciel konta - Administrator Główny - z uprawnieniami administratora, administrator, użytkownik,
- administrator główny jest kontem zarządzającym platformą, zintegrowanym z zewnętrznym serwisem do zarządzania subskrypcją, który jest właścicielem subskrypcji,
- konto administratora głównego nie wlicza się do limitu użytkowników subskrypcji, ma dostęp do wszystkich funkcji platformy. Konta administratora Głównego nie można usunąć, dezaktywować lub obniżyć uprawnień. Edycja danych administratora głównego wymaga zalogowania się do zewnętrznego serwisu do zarządzania subskrypcją,
- administrator jest rolą nadawaną przez administratora głównego lub innego administratora, ma dostęp do wszystkich funkcji platformy, można go usunąć, dezaktywować lub obniżyć uprawnienia

- użytkownik - ma dostęp do swojego pulpitu oraz szkolenia w platformie, nie może zarządzać platformą. Konto użytkownika może zostać utworzone ręcznie przez dowolnego administratora lub zaimportowanie z pliku .CSV.
- możliwość nadania funkcji menedżera grupy - wiąże się z rozszerzeniem widoczności użytkownika o członków grupy, którymi zarządza (wglądu do ich danych, postępów w nauce itd.),
- platforma pozwala na śledzenie postępów użytkowników w kursie (tylko dla Administratorów oraz Menedżerów),
- platforma wyświetla listę aktywności każdego użytkownika w organizacji wraz z informacją o dacie i rodzaju aktywności,
- Administrator ma możliwość podglądu postępu nauki w danym materiale szkoleniowym (lekcja lub test) użytkowników w organizacji,
- Administrator oraz Menedżer mogą pobierać uzyskane przez użytkowników w organizacji certyfikaty.

Właściwości użytkowników:
- imię i nazwisko, e-mail oraz rola (administrator/użytkownik),
- wymóg unikalnego adresu e-mail w obrębie organizacji,
- możliwość dodawania użytkowników do platformy z poziomu interfejsu (formularz),
- możliwość masowego dodawania użytkowników do platformy poprzez import pliku .csv,
- możliwość aktualizacji danych użytkownika (imię i nazwisko) za pomocą importu csv,
- po dodaniu użytkownika do platformy, otrzymuje on wiadomość e-mail z zaproszeniem do organizacji i ustaleniem pierwszego hasła,
- administrator może dowolnie edytować dane wszystkich użytkowników (imię, nazwisko, adres e-mail, rola),
- administrator może dowolnie aktywować oraz dezaktywować konta wszystkich użytkowników,
- administrator może dowolnie usuwać konta wszystkich użytkowników ,
- administrator ma dostęp do wszystkich funkcji w platformie,
- administrator ma dostęp do wszystkich zakładek w platformie,
- użytkownik ma dostęp do zakładki „Pulpit” oraz „Mój kurs”,
- menedżer ma rozszerzony dostęp do grup i użytkowników, którymi zarządza.

Zarządzanie grupami:
- administrator może dowolnie tworzyć, edytować oraz usuwać grupy,
- każda grupa może mieć dokładnie 1 menedżera,
- menedżer nie może edytować grupy, którą zarządza,
- menedżer nie może dodawać lub usuwać użytkowników z grup, którymi zarządza,
- użytkownik może należeć do dowolnej liczby grup,
- menedżer nie musi być członkiem grupy, którą zarządza.

Zarządzanie treścią:
- platforma pozwala na globalne włączanie lub wyłączanie materiałów edukacyjnych,
- wyłączać/włączać można całe moduły, testy z zagadnień, testy końcowe oraz własne materiały,
- platforma pozwala na nieograniczone dodawanie własnych materiałów,
- materiały własne składają się z następujących elementów: nazwa lekcji, szacunkowa długość materiału, miniaturka (widoczna na liście materiałów), osadzone nagranie video, treść materiału – w formie tekstowej, możliwość formatowania treści, osadzenia linków oraz obrazków,
- platforma powinna pozwalać na zmianę kolejności na liście, edytowanie oraz usuwanie własnych materiałów,
- możliwość podejrzenia postępu nauki w konkretnym materiale edukacyjnym użytkowników w organizacji.

Ustawienia organizacji:
- konfiguracja procentowego progu zdawalności testu,

- konfiguracja czasu przed kolejnym podejściem do testu,
- konfiguracja minimalnego wymaganego postępu w kursie (liczba ukończonych materiałów na tydzień),
- informacja o rodzaju subskrypcji (pełna/demo),
- informacja o czasie pozostałym do wygaśnięcia subskrypcji,
- wykres limitu użytkowników (użytkownicy w organizacji/limit subskrypcji).

Inne:
- platforma posiada dedykowaną i stale aktualizowaną Bazę Wiedzy, w której znajdują się artykuły objaśniające najważniejsze funkcje platformy,
- motyw ciemny/jasny,
- comiesięczny newsletter dla użytkowników organizacji (wysyłany na adres e-mail użytkowników).

Wspierane przeglądarki:
- Google Chrome,
- Firefox,
- Microsoft Edge.

Licencjonowanie:
- platforma jest udostępniania w formie płatnego dostępu do usługi on-line w chmurze,
- dostępna w modelu subskrypcyjnym w ramach indywidualnych uzgodnień,
- licencjonowanie usługi obejmuje uzgodniony w ofercie okres czasu (standardowo okres 12- miesięcy) na określoną liczbę dostępów (użytkownicy platformy).

Korzystanie z platformy wymaga utworzenia konta organizacji zgodnie z zasadami wskazanymi w regulaminie platformy.
Po zakończeniu okresu świadczenia usługi Zamawiający lub Usługobiorca będzie mógł zamówić dostęp na nowy okres (przedłużenie świadczenia usługi).
Brak przedłużenia usługi na kolejny okres ze strony Zamawiającego/Usługobiorcy może skutkować blokadą dostępu do konta, a następnie usunięcia konta zgodnie z regulaminem.
Istnieje możliwość rozszerzenia subskrypcji w ciągu roku tj. dokupienia dodatkowych użytkowników w zależności od pozostałych miesięcy do końca ważności dostępu (subskrypcji).
Usunięcie użytkownika skutkuje usunięciem jego danych i historii szkoleniowej.