IZP.271.1.8.2023

Załącznik nr 6 opis przedmiotu zamówienia

Opis przedmiotu zamówienia

1. Stacje robocze – ilość 5 sztuk

Nazwa	Wymagane parametry techniczne
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Przekątna Ekrenu	15,6" FHD (1920 x 1080), powłoką przeciwodblaskową, jasność 250 nits, kontrast min. 700:1, gama koloru min. NTSC 45% (typowo)
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych. Oferowany komputer musi osiągać w teście wydajności : SYSMARK 25 Overall Rating – wynik min. 1200 pkt – test w oferowanej konfiguracji załączyć do oferty. Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.
Pamięć RAM	16GB DDR4 3200MHz możliwość rozbudowy do min 32GB, dwa wymienne sloty na pamięci RAM.
Pamięć masowa	512GB NVMe SSD M.2
Karta graficzna	Zintegrowana karta graficzna osiągająca w teście PC Mark 10 Digital Content Creation co najmniej 3600 punktów – test w oferowanej konfiguracji załączyć do oferty.
Klawiatura	Klawiatura w standardzie US i wbudowanym w klawiaturze podświetleniem, (układ US), min 98 klawiszy. Wszystkie klawisze funkcyjne typu: regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. Nie dopuszcza się innego układu a w szczególności między klawiszami ALT i CTRL (oprócz klawisza FN i Windows z lewej strony)

Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W. Kamera internetowa z diodą informującą o aktywności, 0.9 Mpix, trwale zainstalowana w obudowie matrycy opatrzona wbudowaną mechaniczną przysłonę. czytnik kart microSD, 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Wi-Fi 6 AX201 2x2 + Bluetooth 5.1
Bateria i zasilanie	Bateria Polymer min. 3-cell [min. 45Whr]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Czas pracy na baterii min 9 godzin, potwierdzony przeprowadzonym testem MobileMark25 – test załączyć do oferty. Zasilacz o mocy min. 45W
Waga i wymiary	Waga 1,9kg wraz z baterią. Suma wymiarów notebooka nie większa niż 630mm.
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Komputer spełniający normy MIL-STD-810H w zakresie min. 7 method [załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz oficjalnymi dokumentami producenta komputera]
BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag. Możliwość ustawienia hasła dla administratora, możliwość ustawienia hasła systemowego/użytkownika które jednocześnie będzie blokować uruchamianie systemu z jakichkolwiek urządzeń oraz umożliwia zalogowanie się do BIOS w celu zmiany swojego hasła, możliwość ustawienia hasła dla dysku NVMe, możliwość konfiguracji zależności między tymi hasłami, hasła muszą umożliwiać zawarcia w sobie znaków specjalnych, liczb i liter, Możliwość odczytania informacji o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS , po nadaniu numeru pole nie może być edytowalne.
Certyfikaty	Certyfikat ISO 9001 dla producenta sprzętu (należy załączyć do oferty) Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty) Deklaracja zgodności CE (załączyć do oferty) Certyfikat ISO 50001(należy załączyć do oferty)

	Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony) EnergyStar – załączyć do oferty certyfikat lub wydruk z strony.
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia: dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.
System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny umożliwiający instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.
Oprogramowanie dodatkowe – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające : - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji : a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.

	- rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Porty i złącza	Wbudowane porty i złącza: 1x HDMI 1.4, 1x RJ-45, 2x USB 3.2 (w tym jeden zasilaniem), 1x USB 3.2 TYP-C z obsługą DP 1.2 i zasilaniem, 1x USB 2.0, port zasilania (nie zajmujący portów USB typ C), złącze linki zabezpieczającej.
Warunki gwarancyjne, wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) 3-letnia gwarancja świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta.

2. Stacje robocze – 17 sztuk

Nazwa komponentu	Wymagane parametry techniczne komputerów
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych. Oferowany komputer musi osiągać w teście wydajności : SYSMARK 25 Overall Rating – wynik min. 1500 pkt – test w oferowanej konfiguracji załączyć do oferty. Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.
Pamięć RAM	16GB DDR4 3200MHz. Możliwość rozbudowy do min 64GB.
Pamięć masowa	Dysk M.2 SSD 512GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”.
Wydajność grafiki	Zintegrowana karta graficzna osiągająca w teście PC Mark 10 Digital Content Creation co najmniej 4000 punktów – test w oferowanej konfiguracji załączyć do oferty.
Wyposażenie multimedialne	Karta dźwiękowa min. dwukanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo.
Obudowa	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25” typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 mm. Zasilacz o mocy min. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku, kiedy u producenta występuje kilka

	zasilaczy które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy. Wydruki 80plus musza być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera, iż wskazane zasilacze przez wykonawcę spełniają 80plus. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową

	(wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Funkcja włączająca przypomnienie o konieczności oczyszczenia lub zastąpienia filtra powietrza w jednej z opcji dostępnych: co 15 dni, co 30 dni, co 60 dni, co 90 dni, co 120 dni, co 150 dni i co 180dni Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Wirtualizacja	Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głowej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
System operacyjny	Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny umożliwiający instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.
Certyfikaty i standardy	Certyfikat ISO 9001 dla producenta sprzętu (należy załączyć do oferty) Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty) Deklaracja zgodności CE (załączyć do oferty) Certyfikat ISO 50001 (należy załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony) EnergyStar – załączyć do oferty certyfikat lub wydruk z strony.
Wymagania dodatkowe	Wbudowane porty: 1 x HDMI 1.4 1 x DisplayPort 1.4 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: Panel przedni: 2 x USB 3.2 Typu A oraz 2 x USB 2.0 Panel tylny: 2 x USB 3.2 Typu A oraz 2 x USB 2.0 1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu 1 x RJ – 45 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika),

	Karta WLAN 2x2 802.11ax z Bluetooth w wersji nie niższej niż 5.0 montowana w dedykowanym slocie M.2 na płycie głównej. Nie dopuszcza się kart zajmujących slot PCIe. Płyta główna dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz laserowa USB z sześcioma klawiszami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji	Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata, z możliwością odpłatnego przedłużenia tego okresu do 4 lub 5 lat od daty dostawy. Sposób realizacji usług wsparcia technicznego: Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. Dedykowany bezpłatny portal online producenta do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. Opcjonalna pomoc techniczna za pośrednictwem czat online. Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzien roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Mozliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Dodatkowe oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Wykonawca dostarczy wraz z komputerem oprogramowanie producenta komputera które umożliwia pełne zarządzanie, monitoring, konfigurację a w szczególności: dystrybucję ustawień BIOS (zawierającego wcześniej zdefiniowane ustawienia jednakowe dla wszystkich), jednocześnie na wszystkich komputerach zgodnie z polityką bezpieczeństwa Zamawiającego. Oprogramowanie musi w pełni integrować się z Microsoft SCCM Wykonawca dostarczy sterowniki w formacie dedykowanym dla Microsoft SCCM w celu dystrybucji za pomocą dołączonego oprogramowania producenta komputera zgodnie z polityką bezpieczeństwa Zamawiającego. Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:

	upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o: poprawkach i usprawnieniach dotyczących aktualizacji dacie wydania ostatniej aktualizacji priorytecie aktualizacji zgodności z systemami operacyjnymi jakiego komponentu sprzętu dotyczy aktualizacja wszystkich poprzednich aktualizacjach z informacjami jak powyżej. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.

3. Monitory – ilość 17 sztuk

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
1.	Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą LED, IPS lub VA 21,5"
2.	Jasność	250 cd/m2
3.	Kontrast	1000:1
4.	Kąty widzenia (pion/poziom)	178/178 stopni

5.	Czas reakcji matrycy	max 9 ms
6.	Rozdzielczość maksymalna	1920 x 1080 przy 60Hz
7.	Wyświetlane kolory	16.7 milionów
8.	Zakres pochylenie monitora	+20°~-5°
9.	Powłoka powierzchni ekranu	Antyodblaskowa
10.	Podświetlenie	System podświetlenia LED
11.	Zużycie energii	Typowo 25W, czuwanie mniej niż 0,5W
12.	Bezpieczeństwo	Monitor musi być wyposażony w tzw. Kensington Slot
13.	Waga	Maksymalnie 4 kg
14.	Złącze	VGA (D-sub) - 1 szt. HDMI - 1 szt.DC-in (wejście zasilania) - 1 szt.
15.	Gwarancja	3 lata gwarancji z czasem reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.
16.	Inne	Odłączana stopa, VESA 100mm Redukcja migotania (Flicker free) Filtr światła niebieskiego Głośniki Stereo

4. Oprogramowanie biurowe – ilość 22 sztuk

Microsoft Office Home & Business (licencja wieczysta)

Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.
2. Wymagania odnośnie interfejsu użytkownika:
a. Pełna polska wersja językowa interfejsu użytkownika.
b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
a. Posiada kompletny i publicznie dostępny opis formatu.
b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
c. Pozwala zapisywać dokumenty w formacie XML.
4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego.
5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.
7. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
a. Edytor tekstów.
b. Arkusz kalkulacyjny.
c. Narzędzie do przygotowywania i prowadzenia prezentacji.
d. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami
i zadaniami).
8. Edytor tekstów musi umożliwiać:
a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
b. Wstawianie oraz formatowanie tabel.
c. Wstawianie oraz formatowanie obiektów graficznych.
d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
f. Automatyczne tworzenie spisów treści.

g. Formatowanie nagłówków i stopek stron.
h. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
j. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.
k. Wydruk dokumentów.
l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
m. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016 i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
p. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
9. Arkusz kalkulacyjny musi umożliwiać:
a. Tworzenie raportów tabelarycznych.
b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML).
e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
g. Wyszukiwanie i zamianę danych.
h. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
k. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
m. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania

Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013, 2016 i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a. Przygotowywanie prezentacji multimedialnych, które będą:
b. Prezentowanie przy użyciu projektora multimedialnego.
c. Drukowanie w formacie umożliwiającym robienie notatek.
d. Zapisanie jako prezentacja tylko do odczytu.
e. Nagrywanie narracji i dołączanie jej do prezentacji.
f. Opatrywanie slajdów notatkami dla prezentera.
g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
j. Możliwość tworzenia animacji obiektów i całych slajdów.
k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016 i 2019.
11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
e. Automatyczne grupowanie wiadomości poczty o tym samym tytule.
f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
i. Zarządzanie kalendarzem.
j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.

k. Przeglądanie kalendarza innych użytkowników.
l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
m. Zarządzanie listą zadań.
n. Zlecanie zadań innym użytkownikom.
o. Zarządzanie listą kontaktów.
p. Udostępnianie listy kontaktów innym użytkownikom.
q. Przeglądanie listy kontaktów innych użytkowników.
r. Możliwość przesyłania kontaktów innym użytkowników.
s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

5. Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS) – ilość 1 szt.

OBSŁUGA SIECI
1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokalizacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.

7. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall.
9. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
10. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

INTRUSION PREVENTION SYSTEM (IPS)
11. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
12. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.
13. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
14. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
15. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej.
16. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
17. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
18. Urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

KSZTAŁTOWANIE PASMA (Traffic Shapping)
19. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
20. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
21. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).

22. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

23. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
24. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
25. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
26. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

OCHRONA ANTYSPAM

27. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
28. Ochrona antyspam ma działać w oparciu o:
a. białe/czarne listy,
b. DNS RBL,
c. heurystyczny skaner.
29. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
30. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWANTE (VPN)

31. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
32. Odpowiednio kanały VPN można budować w oparciu o:
a. PPTP VPN,
b. IPSec VPN,
c. SSL VPN
33. SSL VPN musi działać w trybach Tunel i Portal.
34. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.

35. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
36. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
37. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

FILTR DOSTĘPU DO STRON WWW
38. Urządzenie ma posiadać wbudowany filtr URL.
39. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
40. Administrator musi mieć możliwość dodawania własnych kategorii URL.
41. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
42. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
43. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
a. blokowanie dostępu do adresu URL,
b. zezwolenie na dostęp do adresu URL,
c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

44. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
46. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
47. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
48. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE
49. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
a. lokalną bazę użytkowników (wewnętrzny LDAP),
b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
c. usługę katalogową Microsoft Active Directory.
50. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.
51. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia

autoryzacje w oparciu o protokoły:
a. SSL,
b. Radius,
c. Kerberos.
52. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.
53. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
54. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)
55. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
56. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
a. równoważenie względem adresu źródłowego,
b. równoważenie względem połączenia.
57. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

58. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
59. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
60. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
61. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
62. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA
63. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
64. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.

65. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
66. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS
67. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
68. Urządzenie musi posiadać usługę DNS Proxy.

ADMINISTRACJA URZĄDZENIEM
69. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
70. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
71. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
72. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
73. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.
74. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
75. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
76. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
77. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.
78. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
79. Urządzenie musi posiadać funkcjonalność anonimizacji logów.

RAPORTOWANIE
80. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

81. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
82. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB,

modułu IPS, skanera Antywirusowego i Antyspamowego.
83. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów.
84. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
85. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
86. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy

PARAMETRY SPRZĘTOWE
87. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
88. Liczba portów Ethernet 10/100/1000Mbps – min.8.
89. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
90. Przepustowość Firewall – min. 2 Gbps.
91. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – min. 1.6 Gbps.
92. Przepustowość filtrowania Antywirusowego – min. 400 Mbps.
93. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 350 Mbps.
94. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 50.
95. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20.
96. Obsługa min. VLAN 64.
97. Liczba równoczesnych sesji - min. 200 000 i nie mniej niż 15000 nowych sesji/sekundę.
98. Urządzenie jest nielimitowane na użytkowników.
99. Urządzenie musi mieć możliwość utworzenia 4096 reguł filtrowania.
100. Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów.
GWARANCJA I LICENCJA
101. Urządzenie ma być objęte 2 letnią gwarancją oraz aktualizacjami firmware i sygnatur.

6. Zakup specjalistycznego oprogramowania – 28 sztuk

System chroniący przed zagrożeniami, posiadający certyfikaty: OPSWAT Platinum, AV-Test ‘Top Product’, AV Comperative Advance +, ISO 27001 . Silnik musi umożliwiać co najmniej:

- wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
- wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
- stosowanie kwarantanny,
- wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
- skanowanie urządzeń USB natychmiast po podłączeniu,
- automatyczne odłączanie zainfekowanej końcówki od sieci,
- skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
- Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.
- Musi posiadać moduł ochrony IDS/IPS
- Musi posiadać mechanizm wykrywania skanowania portów
- Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
- Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości

Szyfrowanie danych:

- Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.
- Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.

Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.
Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.

Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.
Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware
Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:

- Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli
- Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory
- Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux
- Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.
- Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich
- Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji

Zarządzanie przez Chmurę:

1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach
2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury
3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur
4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy

5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach
6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej

Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.

1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer
2. Oprogramowanie klienckie, zarządzane z poziomu serwera.

System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:

- różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
- funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD
- funkcje regulowania połączeń WiFi i Bluetooth
- funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
- funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi
- funkcje blokowania dostępu dowolnemu urządzeniu
- możliwość tymczasowego dodania dostępu do urządzenia przez administratora
- zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu
- możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
- możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora
- możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry
- możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich
- funkcję wirtualnej klawiatury
- możliwość blokowania każdej aplikacji
- możliwość zablokowania aplikacji w oparciu o kategorie
- możliwość dodania własnych aplikacji do listy zablokowanych
- zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze

- dodawanie innych aplikacji
- dodawanie aplikacji w formie portable
- możliwość wyboru pojedynczej aplikacji w konkretnej wersji
- dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB
- kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
- możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.
- możliwość zablokowania funkcji Printscreen
- funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx
- funkcje monitorowania i kontroli przepływu poufnych informacji
- możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików
- możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj
- możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe
- ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe
- ochrona zawartości schowka systemu
- ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
- możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
- ochrona plików zamkniętych w archiwach
- Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
- możliwość tworzenia profilu DLP dla każdej polityki
- wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
- ochrona przez wyciekiem plików poprzez programy typu p2p

Monitorowanie zmian w plikach:

- Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
- Funkcje monitorowania określonych rodzajów plików.
- Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
- Generator raportów do funkcjonalności monitora zmian w plikach.
- możliwość śledzenia zmian we wszystkich plikach
- możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
- możliwość definiowana własnych typów plików

Optymalizacja systemu operacyjnego stacji klienckich:

- usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku

- optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
- możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich
- instruktaż stanowiskowy pracowników Zamawiającego
- dokumentacja techniczna w języku polskim

Wspierane platformy i systemy operacyjne:

1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)
2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)
3. Mac OS X, Mac OS 10
4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat

Platforma do zarządzania dla Android i iOS:

- Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę
- Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.

Zarządzanie użytkownikiem

- Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email
- Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika
- Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi
- Musi posiadać możliwość eksportu danych użytkownika

Zarządzanie urządzeniem

- Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO
- Musi umożliwiać import listy urządzeń z pliku CSV
- Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych
- Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta
- Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał
- Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres
- Musi zawierać podgląd aktualnie zainstalowanych aplikacji

- Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,
- Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł
- Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres

Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:
Wymagania dotyczące technologii:

1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową
2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.
3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:

- Microsoft Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących
5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:

- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

7. Portal zarządzający musi umożliwiać:

a) przegląd wybranych danych na podstawie konfigurowalnych widgetów
b) zablokowania możliwości zmiany konfiguracji widgetów
c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.
d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
e) eksport wszystkich skanów podatności do pliku CSV

Backup i przywracanie danych

- Deduplikacja danych,

- Backup przyrostowy i różnicowy,
- Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
- Backup danych lokalnych – plikowy oraz poczty Outlook,
- Backup otwartych plików (VSS),
- Filtr plików oraz folderów,
- Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),
- Wyłączanie komputera po wykonaniu backupu,
- Przywracanie danych do wskazanej lokalizacji,
- Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,
- Wyszukiwanie plików w repozytorium użytkownika,

Ustawienia

- Automatyczne logowanie,
- Zapamiętywanie danych logowania,
- Automatyczne uruchamianie programu przy starcie systemu,
- Ustawianie priorytetu dla procesu backupu,
- Zmiana klucza szyfrującego,
- Ustawienia przepustowości/zajętości pasma,
- Konfiguracja wydajności procesu backupu,

Bezpieczeństwo

- Zastępowanie nazwy pliku GUID-em,
- Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,
- Kompresja danych,
- Transmisja po bezpiecznym protokole TLS,
- Deklaracja klucza szyfrującego dane użytkownika,
- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,
- Obliczanie sumy kontrolnej,
- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.

WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji.

7. Zakup specjalistycznego oprogramowania – ilość 22 sztuk

Wymagania ogólne dla systemu zarządzania

Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.

Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .

Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie przypisywania wybranych jednostek organizacyjnych, Jednostek lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty.

Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).

Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.

Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).

Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.

Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).

Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.

Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.

Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.

Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.

Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.

Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.

Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.

Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej

aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień, predefiniowane atrybuty komputera.

Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.

Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.

Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.

Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

Inwentaryzacja konfiguracji komputerów

Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.

Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.

Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.

Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417

Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.

Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.

Oprogramowanie musi umożliwiać analizę sprzętową:

- płyty głównej w zakresie model, producent, nr. seryjny,

- CPU w zakresie nazwy, modelu, producenta, częstotliwości,

- HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,

- RAM w zakresie wielkości pamięci,

- karty sieciowej w zakresie model, adres IP, adres MAC,

- karty graficznej w zakresie model.

Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.

Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.

Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.

Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.

Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.

Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.

Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

Inwentaryzacja oprogramowania

Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
Oprogramowanie musi umożliwiać okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów.
Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

Zarządzanie licencjami, audyt oprogramowania

Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania

Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe).
Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

Zarządzanie zasobami oraz użytkownikami

Oprogramowanie musi umożliwiać klonowanie wybranych typów zasobów
Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
Oprogramowanie musi umożliwiać zdefiniowanie dodatkowych atrybutów dla wybranych relacji pomiędzy zasobami w zakresie zgodnym z atrybutami typów zasobów.
Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.

Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.
Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu.
Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.

Zdalny pulpit, zdalne zarządzanie komputerem

Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).

Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.
Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Automatyzacja

Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie

dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.
Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.
Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.

Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.

Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.

Oprogramowanie musi umożliwiać optymalizację dystrybucji zadań oraz plików na komputery, pobierając brakujące fragmenty plików od agentów z tej samej podsieci (mechanizm peer-to-peer).

Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:

1. Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
2. Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
3. Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi
4. Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
5. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.

W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.

Backup danych użytkownika

Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.

Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.
Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

Zarządzanie urządzeniami USB Storage

Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.
Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage
Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

Monitoring użytkowników

Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.

Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.

Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.

Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

ServiceDesk – Zarządzanie zgłoszeniami

Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:

- Zarządzanie problemem
- Zarządzanie incydentem
- Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
- Zarządzanie umowami serwisowymi
- Definicje poziomów SLA (reakcja, naprawa, reklamacja)

Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.

Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.

Portal ServiceDesk musi zostać dostarczony w technologii PHP w formie otwartych źródeł z możliwością samodzielnej edycji kodu.

Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).

Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.

Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.

Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.

Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.
Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.
Oprogramowanie musi umożliwiać edycję kilku zgłoszeń jednocześnie po wyborze z listy zgłoszeń.
Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
Oprogramowanie musi umożliwiać tworzenie szablonów zadań.
Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.
Oprogramowanie musi umożliwiać administratorowi ustalanie statusów i priorytetów z zaznaczeniem, które z nich może używać użytkownik zgłaszający problem.

Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.

Oprogramowanie musi umożliwiać obsługę autoryzacji OAuth 2.0 w zakresie powiadomień mailowych oraz rejestracji zgłoszeń drogą mailową.

Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.

Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.

Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.

Oprogramowanie musi umożliwiać określenie widoczności poszczególnych statusów i priorytetów w zależności od zalogowanego użytkownika.

Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.

Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.

Zapisane przez administratora rozwiązania incydentów tworzą bazę wiedzy (powiązaną z kategoriami) Baza ta wyświetlana jest użytkownikom podczas przeglądania kategorii zgłoszeń. Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.

Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.

Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefonicznie informuje, że zepsuł mu się komputer).

Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).

Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk.

Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.
Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.
Oprogramowanie musi umożliwiać dostęp lub ograniczenie dostępu do ogłoszeń lub bazy wiedzy dla anonimowego użytkownika.
Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). Możliwość powiązania każdej umowy z zakupionymi licencjami oprogramowania lub z zakupionym sprzętem.
Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.
Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).
Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.

Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)

Oprogramowanie musi umożliwiać klonowanie zgłoszeń.

Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:

- Zmiana statusu po przejęciu zgłoszenia przez opiekuna.
- Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna.
- Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia.
- Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika.
- Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika.
- Zamykanie zgłoszenia po upływie czasu reklamacji.
- Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów.
- Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.
- Walidacja zamkniętych zadań w zamykanym zgłoszeniu.
- Systemowe potwierdzanie realizacji zgłoszenia.
- Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.

Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.

Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.

Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.

Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW operatora HelpDesk informacji nt. aktywności zarejestrowanych stanowisk (on-line/off-line) oraz alertów dotyczących obciążenia CPU, RAM, HDD.

Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).

ServiceDesk – Zarządzanie nieobecnościami

Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.
Oprogramowanie musi umożliwiać zgłaszanie nieobecności użytkowników w wybranych kategoriach z możliwością wykorzystania obiegu zgłoszenia celem akceptacji nieobecności.
Oprogramowanie musi informować o możliwych konfliktach podczas rejestracji nieobecności przez administratorów.
Oprogramowanie musi umożliwiać wgląd w nieobecności podwładnych przez przełożonego.
Oprogramowanie musi podpowiadać aktywne nieobecności w momencie wyboru użytkowników i opiekunów podczas rejestracji i obsługi zgłoszenia.

ServiceDesk – Zarządzanie wnioskami

Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).
Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.
Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.

ServiceDesk – Zarządzanie uprawnieniami

Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych
Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych
Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)

Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek
Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika

ServiceDesk – Zarządzanie rezerwacjami

Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.
Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.
Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.

Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

Monitoring sieci LAN

Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony
Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.
Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

System wewnętrznego komunikatora dla użytkowników

Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.
Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostrgeSQL
Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.
Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami
Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.
Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.
Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).
Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.
Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).
Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.
Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.
Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).
Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami

Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.

Wymagania formalne:

Dostarczone licencje na oprogramowanie muszą być bezterminowe.
Dostarczone licencje na oprogramowanie muszą być dostarczone z 12 miesięcznym supportem producenta, liczonym od daty zakończenia wdrożenia. Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
Dostarczone licencje na oprogramowanie muszą objąć co najmniej 50 stanowisk komputerowych z systemem klasy Microsoft Windows, Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencje dostępową do konsoli zarządzającej
W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.
Zamawiający wymaga od wykonawcy, aby w terminie 10 dni od podpisania umowy przeprowadził wdrożenie systemu zdalnie (wymagana co najmniej 1 sesja – 5 godzinna)
Zamawiający wymaga od wykonawcy, aby w terminie 15 dni od podpisania umowy przeprowadził szkolenie z obsługi systemu zdalnie (wymagana co najmniej 1 sesja – 2 godzinna)

8. Szkolenia dla urzędników w zakresie cyberbezpieczeństwa – ilość 1

W ramach zadania wykonawca przeprowadzi szkolenia w zakresie cyberbezpieczeństwa dla pracowników Urzędu Miejskiego w Dąbiu - szkolenia dla 22 pracowników.
Szkolenia przeprowadzone będą w siedzibie zamawiającego.
Wykonawca przekaże harmonogram szkolenia nie później niż 7 dni przed rozpoczęciem szkolenia.

Program szkolenia:
1. System cyberbezpieczeństwa
• Podstawowe narzędzia cyberbezpieczeństwa
• Z czego powinien składać się skuteczny system cyberbezpieczeństwa
• Jak go zbudować?
2. Podejrzane urządzenia elektroniczne
• Przykłady zagrożeń laptopy, pendrive, smartfony
• Jak się przed tym chronić?
3. Ransomware
• Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
• Jak się chronić i na co zwracać uwagę aby nie paść ofiarą cyberprzestępców
4. Phishing jak działa i na co zwracać uwagę
• Phishing – czym jest, jak działa?
• Przykłady zagrożeń związanych z Phishingem
5. Typowe zagrożenia występujące w internecie
• Prezentacja z wykorzystanie symulatora zagrożeń internetowych

Wykonawca podczas szkoleń zapewni dostęp do nowoczesnej platformy w formie strony www dostępnej w standardzie WCAG 2.1 – symulator zagrożeń internetowych. Szkolenia obędą się z wykorzystaniem dostarczonych komputerów przenośnych – laptop. Symulator musi być narzędziem umożliwiającym użytkownikowi w bezpieczny sposób sprawdzenie oraz poznanie typowych zagrożeń czyhających na użytkowników w Internecie. Korzystanie z symulatora musi być całkowicie bezpieczne dla użytkownika końcowego (żadne z wpisywanych danych nie mogą być zapisywane i archiwizowane). W symulatorze konieczne jest zaimplementowanie min. 8 scenariuszy (zagrożeń) popularnych przestępstw internetowych, z którymi użytkownicy mogą się spotkać podczas codziennego korzystania z Internetu. Pierwsze cztery dotyczące tzw. Phishing'u w różnych odsłonach, ((Phishing Clone, Phishing Spear, Phishing Spear Chat, Phishing Whaling) następny dotyczy oszustwa typu Pharming, dwa kolejne mają przedstawiać zasadę działania zagrożenia typu Malware, (Malware Post, Malware Email,) natomiast ostatni dotyczący certyfikatów SSL (Certificate Fraud Chat) . Wykonawca zobowiązany jest przekazać zamawiającemu dostępy do platformy na min 30 dni od daty szkolenia, wraz z instrukcją obsługi. Wymagania szczegółowe dla platformy Symulującej zagrożenia internetowe:
a) Moduł podstron (fałszywych witryn) – moduł ten będzie umożliwiał tworzenie różnego rodzaju fałszywych witryn nakłaniających użytkowników do pobierania zainfekowanych

załączników, podawania danych wrażliwych i/lub dokonywania płatności internetowych.
b) Moduł czatu – w module tym zaimplementowany zostanie czat z botami, namawiającymi do zakupów różnych produktów powodując wyłudzenie danych osobowych, numerów kart kredytowych itp. Itd. W module tym zostaną zaimplementowane opracowane scenariusze
c) Moduł e-mail – w module tym użytkownik będzie miał do przeglądnięcia kilka wiadomości e-mail przesłanych z różnych źródeł, wiadomości te będą zawierały linki bądź załączniki po kliknięciu których, zostanie uruchomiona akcja symulująca zachowanie się malware, np. blokada komputera (przeglądarki) na jakiś określony czas. Po kliknięciu załącznika „zainfekowanego" na ekranie powinna pojawić się informacja na temat, że twój komputer został zainfekowany, wykradliśmy twoje dane osobowe itd. Itp. W tym module należy również pokazać działanie tzw. szyfrującego wirusa, który po kliknięciu w załącznik szyfruje wszystkie pliki tekstowe, w tym przypadku symulator powinien pokazać przykład
d) Moduł edukacyjny – moduł zawierający szczegółowe informacje na temat występujących cyberprzestępstw. W szczególności powinien się skupić na phishingu, pharmingu oraz malware.
✓ Moduł ten powinien zawierać informacje na temat występowania oraz identyfikacji danego zagrożenia, sposobów zapobiegania, oraz informacji na temat, co użytkownik powinien w pierwszej kolejności zrobić, gdy zostanie już oszukany – czyli gdzie się zgłosić najpierw, jakie dane zabezpieczyć, zmienić hasła, czy zablokować karty płatnicze.
✓ Materiały edukacyjne powinny być przedstawione w formie plików PDF przedstawiających, na co zwrócić szczególną uwagę podczas korzystania z portali społecznościowych, różnego rodzaju czatów, różnego rodzaju serwisów internetowych oraz odbierania wiadomości e-mail.
✓ Moduł edukacyjny powinien być ściśle zintegrowany z pozostałymi modułami tj. Po przejściu każdego z opracowanych i zaimplementowanych w symulatorze scenariuszy powinna pojawić się informacja o tym jak i dlaczego użytkownik dał się oszukać i jakie to może mieć konsekwencje w późniejszym czasie.
e) Moduł postów społecznościowych, zawierający możliwe ataki phishingowe lub pharmingowe, w module postów społecznościowych będą znajdować się zarówno „rzeczywiste" posty nie stanowiące zagrożenia jaki i posty z potencjalnym zagrożeniem.