Załącznik nr 1 do SIWZ

I. Serwer z oprogramowaniem – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji 8 dysków 2.5" wraz z kompletem szyn umożliwiających montaż w szafie rack. Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp poprzez urządzenia mobilne; Serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów przy użyciu dedykowanej aplikacji mobilnej min. (Android/ iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Umożliwiająca zainstalowanie dwóch procesorów. Zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Procesory	Zainstalowane dwa procesory, z których każdy musi oosiagać w teście PassMark CPU Mark wynik 25 200 – **załączyć do oferty wydruk ze strony https://www.cpubenchmark.net/**
Pamięć RAM	128 GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s. Na płycie głównej powinno znajdować się min. 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać 1TB pamięci RDIMM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Interfejsy sieciowe/FC/SAS	Zainstalowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT nie zajmujące slotu PCIe
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 4 dyski SSD o pojemności 480GB każdy, 6Gb/s, 2,5“ Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności 480GB z możliwością konfiguracji RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy, umożliwiający konfiguracje poziomów RAID: 0, 1, 10. Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	Przednie: 1 x VGA, 1 x USB 3.0, 1 x micro-USB dedykowane dla karty zarządzającej, Tylne: 1 x VGA, 2 x USB w tym 1 x USB 3.0, Nie dopuszcza się stosowania konwerterów/przejściówek.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości 1600 x 900;
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug. 800W, o sprawności 94% przy 50% obciążeniu. Dołączone dwa kable zasilające PDU Rack o długości min. 2m
System operacyjny	System operacyjny w najnowszej wersji spełniający poniższe wymagania: 1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

	2. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 3. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 4. Czterdziesci licencji dostępowych do usług serwera dla urządzeń znajdujących się w sieci zamawiającego; 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 9. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 10. Możliwość uruchamianie aplikacji internetowych wykorzystujących techologię ASP.NET. 11. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 12. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 13. Graficzny interfejs użytkownika. 14. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 15. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 16. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 17. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 18. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). 19. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na

	tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. e) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: dystrybucję certyfikatów poprzez http, konsolidację CA dla wielu lasów domeny, automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6). k) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerac;, l) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. m) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath); n) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. o) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. p) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WSManagement organizacji DMTF; q) Materiały edukacyjne w języku polskim. 20. Licencja na 16 rdzeni procesorowych; 21. Analizator najlepszych praktyk 22. Pamięć dynamiczna przy wirtualizacji; 23. Dodawanie i wymiana kości RAM bez wyłączania systemu operacyjnego; 24. Konsola zarządzająca; 25. Sieciowy load balancing; 26. Migracja pamięci masowej; 27. Aktywacja zbiorcza; 28. Manager zasobów systemu operacyjnego; 29. Logowanie licencji serwera; 30. Nieograniczona liczba połączeń RRAS; 31. Obsługa 64 gniazd 64 bitowych; 32. Obsługa 24 TB pamięci RAM; 33. Możliwość dołączenia do domeny; 34. Kodeki DLNA i strumieniowe przesyłanie multimediów internetowych; 35. Certyfikaty usług katalogowych;

	36. Zarządzanie usługami katalogowymi; 37. Serwer: DHCP, DNS, iPAM, iSNS, SMTP, faksów, plików, dla NFS; 38. Deduplikacja danych 39. Replikacja systemu plików DFS; 40. Funkcja serwera docelowego iSCSI I kontrolera sieci; 41. Możliwość dostępu i pulpitu zdalnego; 42. Usługi IIS; 43. Usługa inteligentnego transferu w tle; 44. Szyfrowanie I odblokowywanie dysków bitlocker; 45. Możliwość pracy w klastrze; 46. Zarządzanie politykami grupowymi; 47. Monitorowanie portów LPR; 48. Kolejkowanie wiadomości; 49. Protokół rozpoznawania nazw równorzędnych; 50. Manager połączeń RAS; 51. Zdalna pomoc użytkownikom sieciowym; 52. Zdalna kompresja różnicowa; 53. RSAT; 54. RPC przez proxy HTTP; 55. Usługi TCP/IP; 56. Udostępnianie plików SMB 1.0/CIFS; 57. Klient Telnet i TFTP; 58. Wewnętrzna baza danych; 59. Kopia zapasowa serwera; 60. Narzędzia do migracji system operacyjnego; 61. Filtr TIFF IF;
Bezpieczeństwo	1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz do ochrony nieautoryzowanego dostępu do dysków twardych. 2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła 4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5. Moduł TPM 2.0 6. Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera 7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Znajdująca/-y się na froncie obudowy panel LCD lub sygnalizacja diodami LED, umożliwiająca/-y wyświetlanie informacji o stanie: temperatury, pamięci RAM, dysków, slotów PCIe
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: 1. monitoring wszystkich kluczowych komponentów (wentylatory, zasilacze, pamięć, procesor, RAID, karty sieciowe oraz dyski twarde) 2. zdalny dostęp do graficznego interfejsu web karty zarządzającej 3. uzyskanie informacji o aktualnym zużyciu energii oraz temperaturach 4. kontrola zasilania (włączenie, wyłączenie, restart) 5. wsparcie dla IPv6

	6. podstawowe funkcje diagnostyczne: podgląd dziennika systemowego, dziennika kontrolera cyklu życia; 7. odtworzenie konfiguracji sprzętowej na podstawie kopii z innego serwera 8. możliwość skonfigurowania wielu kont o zróżnicowanym poziomie przywilejów 9. szyfrowanie protokołem SSL 10. wsparcie dla dynamic DNS
Gwarancja	3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia; Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Uszkodzony dysk twardy pozostaje u Zamawiającego – **załączyć do oferty** oświadczenie producenta serwera, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego; Serwis musi być świadczony zgodnie z normami ISO 9001 i 27001 – **załaczyć do oferty certyfikaty dla oferenta;** Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 **– załaczyć do oferty;** Serwer musi być kompatybilny z oferowanym systemem operacyjnym – **załaczyć do oferty wydruk ze strony producenta oprogramowania**
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

II. Serwer NAS – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Osiągający wynik 1100 pkt w teście PassMark CPU Mark – **załączyć do oferty wynik ze strony www.cpubenchmark.net lub www.passmark.com;**
Pamięć	32 GB;
Pamięc flash	4 GB z ochroną przed podwójnym rozruchem;
Zatoki na dyski	4 szt.;
Obsługiwane dyski	2,5 cala SSD SATA oraz 3,5 cala SATA; hot swap;
Porty	2 x M.2 2280 PCIe Gen 3, 2 x 2,5 GbE, 2 x 10 GbE SFP+, 4 x USB, w tym 2 x USB 3.2;
Obudowa	Maksymalnie 1U rack;
Diody	LAN, USB, zatoki dyskowe, złącza M.2;
Zasilacz	Maksymalnie 100W;
Wentylator	3 x 40 mm;
Połączenia CIFS	1500;

Rozmiar puli	300 TB;
Ilość pul	128
Zainstalowane dyski	4 x 4 TB SATA 6 Gb/s; Pamięc podręczna – 256 MB; Szybkość transferu – 200 MB/s.; CMR; MTBF – 1 min. godzin; Głośność podczas pracy – maksymalnie 28 dBA;
Pobór mocy podczas pracy	Maksymalnie 35W;
System operacyjny	1. Pula pamieci SED; 2. Obsługiwany rozmiar woluminu – 250 TB; 3. Liczba folderów udostpenianych – 512; 4. Rozmiar folderu udostępnianego – 250 TB; 5. Rozszerzenie JBOD; 6. VJBOD; 7. Usługa iSCSI i FC; 8. Jednostka iSCSI LUN oparta na plikach i blokach; 9. Mapowanie LUN; 10. Przenoszenie jednostki LUN między iSCSI i FC; 11. Maskowanie LUN 12. Import/eksport aliasów WWPN 13. Wiązanie portu FC 14. Wielościeżkowe we/wy (MPIO) 15. Rozszerzenie pojemności jednostek LUN online 16. Migawka jednostki LUN 17. Replikacja migawek LUN i klonowanie; 18. Automatyczne poziomowanie; 19. Obsługa RAID - JBOD, RAID 0, 1,5,6,10; 20. Migracja poziomu RAID; 21. Rozszerzenie RAID i puli pamięci; 22. Hot spare RAID; 23. Synchronizacja RAID, odbudowa i czyszczenie; 24. Migawka woluminu i jednostki LUN; 25. 256 migawki na urządzenie i 64 na jednostkę LUN; 26. Interwał migawki – 5 minut; 27. Samoobsługowe odzyskiwanie migawek; 28. Migawka złożona z aplikacji; 29. Pamięć podręczna do odczytu i zapisu; 30. Narzędzie do profilowania SSD; 31. Zarządzanie zewnętrznym urządzeniem RAID; 32. Serwer plików; 33. Serwer FTP; 34. Kontroler domeny; 35. Limitowanie liczby użytkowników; 36. Monitor zasobów; 37. SNMP v2 i 3 38. Odzyskiwanie plików usuniętych ; 39. Automatyczne czyszczenie i filtr typu pliku 40. Dziennik systemowy i centrum powiadomień; 41. Harmonogram włączania i wyłaczania; 42. Przełącznik wirtualny;

	43. Trunkowanie portów; 44. Serwer DHCP;
Gwarancja	2 lata NBD;
Wymagania dodatkowe	Przyspieszenie pamięci SSD, WoL, ramki Jumbo, szyny do montażu w szafie rack 19 cali, złącze Kensingotn,

III. Oprogramowanie do backupu – 1 szt.

Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dla 40 stacji roboczych.

1. Oprogramowanie musi wspierać fizyczne komputery z systemem operacyjnym Windows oraz macOS.
2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
   - Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.
   - Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
   - Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.
   - Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).
   - Zdalna instalacja agentów kopi zapasowych na maszynach z systemem operacyjnym Windows.
   - Zdalne uaktualniania agentów kopi zapasowych.
   - Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.
3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
   - Kopie zapasowe całych dysków i partycji.
   - Kopie zapasowe wybranych plików i folderów.
   - Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.
   - Zapis kopi zapasowych na udziały sieciowe.
   - Zapis kopi zapasowych na serwer SFTP.
   - Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
   - Szyfrowanie plików kopi zapasowych.
   - Wsparcie dla technologii VSS.
   - Kompresja plików kopi zapasowych.
   - Replikacja kopi zapasowych na kolejny nośnik (dysk, magazyn chmurowy).
4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:
   - Odtworzenie całej maszyny (Windows, Mac) – tzw. Bare Metal Restore.
   - Odtworzenie całej maszyny (Windows, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
   - Odtworzenie poszczególnych plików i folderów.
5. Wymagania związane ochroną danych:
   - Ochrona systemów operacyjnych przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.
   - Wbudowana ochrona antywirusowa i antymalware.
   - Mechanizm ochrony przed exploitami.

- Filtrowanie adresów URL.
- Zarządzanie oprogramowaniem antywirusowym;
- Funkcja otrzymywania informacji o nowych zagrożeniach wraz ze wskazaniem zadań do wykonania dla konkretnego zagrożenia (m.in instalacja poprawki, wykonanie skanowania stacji).
- Mechanizm badania zdrowia dysku.
- Mechanizm ciągłej ochrony (backupu) plików zapisywanych w wybranych aplikacji lub lokalizacji. Funkcja ta musi co najmniej wspierać aplikacje z kategorii dokumentów (m.in Office, LibreOffice), inżynierii (Autocad) oraz z możliwością wskazania niestandardowej aplikacji.
- Filtrowanie stron na podstawie kategorii stron.

6. Wymagania co do modelu licencjonowania rozwiązania:
   - Licencja subskrypcyjna na rok lub wieczysta;
7. Zamawiający wymaga aby wdrożenie i szkolenie dostało wykonane przez firmę posiadającą uznaną przez producenta oprogramowania pierwszą linię wsparcia w języku polskim.
8. Po wykonaniu wdrożenia zostanie przeprowadzone szkolenie polegające na omówieniu planów ochrony, harmonogramów oraz elementów security, które zostaną uruchomione w ramach licencji;
9. Wdrożenie i szkolenie będzie przeprowadzone w ciągu jednego dnia (8 godzin) w siedzibie zamawiającego.
10. Zakres wdrożenia musi obejmować co najmniej następujące elementy:
    a) Wdrożenie konsoli zarządzania na komputerze w sieci lokalnej
    b) Podpięcie kluczy licencyjnych do konsoli lokalnej lub chmurowej
    c) Instalacja agenta;
    d) Omówienie planów ochrony, ustawienie harmonogramu, przypisanie planu do komputerów, serwerów, hostów wirtualnych,
    e) Dodanie magazynu kopii zapasowych
    f) Ustawienie serwera poczty e-mail dla raportów,
    g) Skonfigurowanie wysyłki raportów,
    h) Dostosowanie ustawień domyślnych do potrzeb zamawiającego;
    i) Ustawienie ochrony baz danych w ramach 1 serwera, jeżeli dotyczy;

IV. System centralnego logowania – 1 szt.

1. Oprogramowanie musi posiadać budowę modułową oraz składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów;
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami musi przebiegać przy użyciu szyfrowanego protokołu TLS;
3. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.
4. Moduły muszą umożliwiać monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z użytkownikiem;
5. Program musi wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source;
6. Baza danych musi być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania;
7. Dane, które dotyczą działań użytkownika na komputerze, takie jak: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych muszą być odseparowane od danych stricte technicznych o stacji roboczej;
8. Musza byc one grupowane w osobnym, dedykowanym oknie;

9. Możliwość zgodne z RODO, usuwania danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej;
10. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych administratorów;
11. Możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień;.
12. Główny Administrator musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną;
13. Działania administratorów muszą być logowane w dzienniku z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta.
14. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog;
15. Monitorowania bezagentowe musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:
    a) wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
    b) wykrywania urządzeń na podstawie informacji odczytanych z Active Directory wraz z informacją o OU;
    c) wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
    d) wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
    e) wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
    f) wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
    g) wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
    h) wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
    i) wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
    j) zablokowania mapy urządzeń przed przypadkową edycją
    k) serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program musi monitorować czas ich odpowiedzi i procent utraconych pakietów
    l) serwerów pocztowych:
    - program musi monitorować czas logowania do serwisu odbierającego oraz czas wysyłania poczty;
    - program musi mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS);
    - program musi mieć możliwość wykonywania operacji testowych i wysłania powiadomienia jeśli serwer pocztowy nie działa
    m) monitorowania serwerów www i adresów URL;
    n) cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
    o) obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
    p) obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją – monitorowanie wartości za pomocą nazw zmiennych oraz OID
    q) obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
    r) monitoring routerów i przełączników według:

- zmian stanu interfejsów sieciowych
- ruchu sieciowego
- podłączonych stacji roboczych – graficzna prezentacja panelu switcha
- ruchu generowanego przez podłączone do portów stacje robocze

s) serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
t) wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
u) wydajności sytemów operacyjnych, w tym: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy;

16. Program musi posiadać inteligentne mapy do zarządzania logiczną strukturą urządzeń;
17. Kryteria automatycznego filtrowania dotyczyć muszą: statusu agenta, wygenerowanych alarmów, zainstalowanych aplikacji, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia;
18. Program musi posiadac funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.
19. Program musi umożliwiać nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów, definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie;
20. Alarmy muszą być budowane przez administratora z wykorzystaniem ciągu przyczynowo skutkowego.
21. Administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.
22. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut.
23. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00.
24. Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia;
25. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0;
26. Program musi mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP);
27. W zakresie inwentaryzacji program automatycznie musi gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

a) prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart;
b) obejmować zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
c) Informować o zainstalowanych aplikacjach oraz aktualizacjach systemu operacyjnego co musi umożliwiać audytowanie i weryfikację użytkowania licencji w organizacji.
d) zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP;
e) posiadać możliwość wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
f) umożliwiać odczytanie numeru seryjnego;
g) umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.

h) umożliwiać przegląd informacji o konfiguracji systemu, w tym komend startowych, zmiennych środowiskowych, kont lokalnych użytkowników, harmonogramu zadań;
i) umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika;
j) umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji muszą być logowane.

28. Moduł inwentaryzacji zasobów musi umożliwiać:
a) prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i oprogramowania:
b) przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatyczne aktualizowanie zgromadzonych informacji,
c) tworzenie powiązań między zasobami a kontami użytkowników i wskazywanie osób odpowiedzialnych,
d) wskazanie osób uprawnionych do użycia zasobów;
e) definiowanea własnych typów zasobów, ich atrybutów oraz wartości jak np. numer inwentarzowy;
f) określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
g) określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
h) importu danych z zewnętrznego źródła;
i) przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF);,
j) oznaczanie statusów zasobów, np. w użyciu, w naprawie, zutylizowany;,
k) ewidencję czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności;
l) generowanie zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania;
m) przygotowanie szablonów generowanych dokumentów i protokołów przekazania zasobów;,
n) konfigurację automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca;
o) archiwizację i porównywanie audytów zasobów,
p) tworzenie kodów kreskowych dla zasobów,
q) drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy;
r) inwentaryzację zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet;
s) zmianę portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
t) inwentaryzację stacji roboczych niepodłączonych do sieci;,
u) definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji;

29. Inwentaryzacja oprogramowania musi umożliwiać pozyskiwanie informacji o oprogramowaniu i audycie licencji poprzez:
a) skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
b) Informacje o aplikacjach używanych w organizacji.
c) Tworzenie własnych wzorców aplikacji.
d) Tworzenie dowolnych kategorii aplikacji;
e) Informacje o komputerach, na których aplikacja została wykryta.
f) Zarządzanie posiadanymi licencjami.

g) Wskazywanie osób odpowiedzialnych za licencję.
h) Wskazanie użytkowników licencji
i) Scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
j) audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji;
k) zarządzanie posiadanymi licencjami: raport zgodności licencji.
l) możliwość przypisania do programów numerów seryjnych, wartości itp.

30. W zakresie obsługi uzytkowników program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach poprzez monitorowanie:
    a) Faktycznego czasu aktywności - dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy,
    b) Procesów - każdy proces musi mieć całkowity czas działania oraz czas aktywności użytkownika wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
    c) Rzeczywistego użytkowania programów (procentowa wartość wykorzystania aplikacji, obrazujący czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność),
    d) Informacji o edytowanych przez użytkownika dokumentach,
    e) Historii pracy (cykliczne zrzuty ekranowe),
    f) Listy odwiedzanych stron WWW - liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
    g) Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
    h) Wydruków - informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
    i) Nagłówków przesyłanych w aplikacjach klienckich poczty e-mail.
31. Program musi posiadać możliwość:
    a) blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen;
    b) Reguły w postaci listy domen tworzone musza być dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami;
    c) blokowania ruchu na wskazanych portach TCP/IP,
    d) blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
    e) wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,
    f) przygotowania zestawienia ustawień monitorowania użytkownika w postaci raportu;,
    g) definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
32. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
33. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku.

34. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone muszą być dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
35. Program musi posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych;
36. Program musi umożliwiać zdalną pomoc użytkownikom;
37. W ramach kontroli stacji użytkownika dostępny musi być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika
38. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran.
39. Administrator w trakcie zdalnego dostępu musi mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika.
40. Baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz wiadomości e-mail, które musza być przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.
41. Oprogramowanie musi pozwalać na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0.
42. Moduł musi umożliwiać przetwarzanie zgłoszeń w trybie oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych;
43. Umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze;
44. Komunikator, który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami;
45. Czat musi pozwalać na:
    a) zarządzanie dostępem w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
    b) rozmowy również między „zwykłymi" użytkownikami
    c) przesyłanie plików między rozmówcami w trybie online
    d) tworzenie pokojów tematycznych, rozmów grupowych
    e) oznaczanie kontaktów jako „ulubionych" na liście kontaktów
    f) uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
    g) wyświetlanie w trybie jasnym lub ciemnym
46. Baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać, powtarzające się problemy wraz z możliwością nadawania artykułom statusów;
47. Program musi umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy.
48. Dostęp do systemu zgłoszeń oraz bazy wiedzy przez dedykowany portal dostępny przez przeglądarkę internetową;
49. Uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.
50. Moduł pomocy zdalnej umożliwia również:
    a) pobieranie listy użytkowników z Active Directory;
    b) zarządzanie lokalnymi kontami w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,

c) zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń'
d) tworzenie drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach opisami kategorii oraz klauzulą RODO,
e) automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
f) definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
g) procesowanie zgłoszeń użytkowników z wiadomości e-mail,
h) integrację ze skrzynkami e-mail w oparciu o autoryzację login/hasło oraz mechanizm OAuth 2.0,
i) tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
j) wykonywanie operacji na wielu zgłoszeniach równocześnie,
k) wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
l) dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
m) wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
n) zdalną modyfikację rejestrów,
o) definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI;
p) przypisywanie dostępnych instalatorów do grup użytkowników,
q) zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
r) możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
s) obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami;
t) generowanie raportów obsługi helpdesk,
u) zdalne wykonywanie poleceń poprzez Agenty;
v) zarządzania procesami systemu operacyjnego;

51. Ochrona danych przed wyciekiem poprzez blokowanie urządzeń.
52. Blokowanie urządzeń i nośników danych.
53. Program musi mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny;
54. Blokowanie urządzeń i interfejsów fizycznych: USB, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD;
55. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
56. Blokownie musi dotyczyć tylko urządzeń służących do przenoszenia danych. Inne urządzenia (drukarka, klawiatura, mysz) muszą być aktywne;
57. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
58. Integracja i zarządzanie ustawieniami co najmniej aplikacji Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
59. Monitorowanie stanu szyfrowania dysków BitLocker.
60. Monitorowanie stanu modułu TPM;
61. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
62. Autoryzowanie urządzeń firmowych, w tym: szyfrowanych pendrive'ów i dysków. Urządzenia prywatne muszą być blokowane;
63. Blokowanie określonych typów urządzeń dla wybranych użytkowników.
64. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.

65. Możliwość usuwania z listy znanych urządzeń tych nośników, które zostały zutylizowane.
66. Audyt operacji na plikach na urządzeniach przenośnych:
67. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
68. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.
69. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych oraz przydzielanie uprawnień również do kont użytkowników lokalnych;
70. Portal informacyjny w formie platformy www, który pozwala na tworzenie interaktywnych paneli informacyjnych z widgetami.
71. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być:
    a) Udostępniana w trybie „tylko do odczytu" z zabezpieczeniem tokenem.
    b) Wyświetlana w trybie jasnym lub ciemnym;
72. Oprogramowanie musi umożliwiać zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.
73. Widgety muszą prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania, w tym:
    a) Liczniki wydajności, Alarmy oraz odpowiedzi serwisów TCP/IP;
    b) Ostatnie urządzenia podłączone do sieci,
    c) Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów;
    d) Statystyki z obszaru wydruków, Statystki użycia aplikacji;
    e) Statystyki z obsługi zgłoszeń, Lista nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,
74. Program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działaniem i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
75. Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.
76. Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, w tym: urządzenia, użytkownicy, zasoby;
77. Program dostępny musi być w języku polskim i angielskim;

V. Urządzenie wielofunkcyjne – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ urządzenia	Laser lub LED, kolor
Panel LCD	10 cali
Prędkość kopiowania A4 mono i kolor	25 str. A4 minutę
Czas wydruku pierwszej kopii kolor	Maksymalnie 10 sekund
Czas przygotowania do pracy	Maksymalnie 25 sekund
Formaty kopii	A3 – A6
Pojemność kaset na papier A3 i A4	2 x 500 arkuszy
Pojemność podajnika ręcznego	100 arkuszy
Podajnik automatyczny	100 arkuszy
Pojemność tacy wyjścia	250 arkuszy
Funkcje drukarki	Drukowanie sieciowe, PCL 5c; PostScript 3; XPS
Funkcje skanera	Kolorowe skanowanie sieciowe z szybkością 80 stron mono i kolor na minutę, skan do e-mail, FTP, USB, zapis na dysku wewnętrznym; Format wyjściowy skanów: JPEG, TIFF, PDF, Compact PDF, PDF z hasłem, XPS, Compact XPS;

Porty komunikacyjne	1 GbE, USB 2.0
Pamięć	4 GB + wbudowany dysk SSD o pojemności 250 GB
Zabezpieczeni danych na dysku wewnętrznym	- Szyfrowane hasło do dysku twardego; - Hasło administratora do skrzynki;
Materiały eksploatacyjne dostarczone z urządzeniem	Oryginalne tonery producenta urządzenia CMYK na 28 000 stron A4; Bęben/y czarny na 150 000 stron A4 oraz CMY na 60 000 stron A4 każdy; Urządzenia muszą posiadać oryginalne, fabrycznie nowe, nie regenerowane materiały eksploatacyjne (bębny i tonery) producenta urządzenia;
Certyfikaty	Serwis musi być świadczony zgodnie z normami ISO 9001 oraz ISO 27 0001 – **certyfikaty dla oferenta na serwis rozwiązań informatycznych załączyć do oferty;** Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji na rynek polski **– załączyć do oferty oświadczenie producenta;**
OCR	Dostępna z panelu urządzenia funkcja sieciowego OCR o następujących funkcjonalnościach: 1. OCR musi być zintegrowany z wyposażonymi w panel dotykowy urządzeniami; 2. OCR nie może obciążać swoim działaniem komputerów użytkowników i nie może wymagać instalacji dodatkowego oprogramowania; 3. OCR musi umożliwiać pozyskiwanie treści z dokumentów papierowych lub elektronicznych umieszczonych w katalogu sieciowym, a następnie przetwarzać je do elektronicznego pliku w formacie edytowalnym, w tym co najmniej: doc, docx, xls, xlsx lub pdf, pdf/a (z możliwością wyszukiwania tekstu) w języku polskim; 4. OCR musi umożliwiać rozpoznawanie pól i kodów kreskowych; 5. OCR musi umożliwiać rozdzielanie dokumentów za pomocą przekładek w postaci pustych stron; 6. OCR musi umożliwiać rozdzielanie dokumentów za pomocą kodów kreskowych; 7. OCR musi umożliwiać tworzenie plików XLS z zachowywaniem tła komórek, konwersji tekstu na liczby, zachowywanie kolorów tekstu, usuwanie formatowania tekstu, rozpoznawanie tylko tabel; 8. OCR musi umożliwiać tworzenie przeszukiwalnych plików PDF z opcjami, jako tekst nad obrazie, obraz na tekście, tekst i obraz, tylko obraz; 9. OCR musi umożliwiać przesłanie pozyskanej treści dokumentu w postaci pliku, poprzez wiadomość elektroniczną na skrzynkę pocztową użytkownika, bezpośrednio po zakończeniu OCR dokumentu; 10. System musi umożliwiać zdefiniowanie maksymalnego rozmiaru skanowanego pliku

	wysyłanego pocztą e-mail, po przekroczeniu którego dokument zapisywany będzie na lokalnym zasobie sieciowym, a właściciel musi otrzymać wiadomość e-mail zawierającą link w postaci ścieżki URL, z zaszyfrowaną nazwą pliku uniemożliwiającą podejrzenie bezpośredniej lokalizacji pliku. Po jego kliknięciu użytkownik musi otrzymać możliwość otworzenia lub zapisania pliku na dysku lokalnym; 11. OCR musi posiadać licencje na 4000 skanów miesięcznie; 12. OCR nie może posiadać limitu na ilość podłączonych użytkowników;
Funkcja zgłaszania usterek	1. Urządzenie musi umożliwiać wysłanie bezpośrednio z panelu informacji o niepoprawnym działaniu, problemach z jakością wydruków/kopii, oraz innych, które nie mogą być raportowane automatycznie poprzez SNMP;. 2. Rodzaj problemu musi być dostępny do wyboru przez użytkownika w postaci gotowej listy potencjalnych usterek; 3. W przypadku usterki polegającej na złej jakości kopii/wydruku urządzenie musi pozwalać na załączenie do wysyłanej informacji skanu dokumentu, co do którego są zastrzeżenia jakościowe; 4. Wygenerowany w ten sposób alert musi zawierać dodatkowe informacje uzupełnione automatycznie przez urządzenie w postaci: numeru seryjnego urządzenia, daty, godziny;
Wymagania dodatkowe	Dupleks i ADF; Oryginalna podstawa producenta urządzenia na kółkach z szafką; Kabel zasilający 1.8m; Kabel drukarkowy USB 1.8m; Kabel Ethernet 3m.
Warunki gwarancji	3 lata; Cena musi uwzględniać wszystkie przeglądy niezbędne do utrzymania gwarancji; Wykonawca zobowiązany jest w okresie gwarancji do przeprowadzenia co najmniej jednego przeglądu rocznie, obejmującego: - Demontaż i montażu maszyny; - Czyszczenie podzespołów: optyki, poboru i transportu papieru, i wyposażenia opcjonalnego (podajniki dokumentów, separatory itp.); - Aktualizacjję oprogramowania sprzętowego; - Ocenę stanu technicznego urządzenia.

VI. System zasilania awaryjnego – 1 szt.

1. UPS - Typ I – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Rodzaj	jednofazowy
Typ obudowy	Metalowa rack/tower z zestawem montażwym w szafie rack;
Topologia	Line-interactive;
Rodzaj wejścia	Schuko;
Wyjście	6 x IEC C13, 2 x IEC C19; zabezpieczone przed przepięciami i bateriami;
Obciążenie krytyczne i niekrytyczne CL/NCL	4
Czas transferu	Maksymalnie 5 ms.
Przewód zasilający	2,4 m.
Moc VA/W	3000;
AVR	Double Boost, single buck;
Układ przecieprzepięciowy	2400J, ochrona sieci LAN (RJ45),
Czas pracy podtrzymania na baterii	10 minut przy pełnym obciążeniu/ 35 min. przy połowicznym – **załaczyć do oferty dokument potwierdzający autorstwa producenta urządzenia;**
Czas ładowania baterii	Maksymalnie 9h;
Złącza	1 x EPO, 1 x USB, 2 x port szeregowy, 3 x RJ45;
Rozpraszanie ciepła	Maksymalnie 125 BTU/h
Hałas	Maksymalnie 60 dBA;
Warunki gwarancji	2 lata; Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikat załączyć do oferty;** Oferowany zasilacz musi pochodzić z autoryzowanego kanału dystrybucji na rynek polski **– załączyć oświadczenie producenta**
Wymagania dodatkowe	Kompatybilność z aktywnym PFC, zdalne monitorowanie SNMP/HTTP, obrotowy panel LCD, wewnętrzny ogranicznik prądu, bezpiecznik, uruchamianie na baterii, wbudowany moduł zarządzania akumulatorem, możliwość wymiany baterii przez użytkownika, bateria hot-swap, filtrowanie EMI/RFI, styk bezprądowy z przekaźnikiem, TVSS, kabel USB, EPO, szeregowy, 5 x kabel zasilający;, wbudowana ładowarka;

2. Przełącznik serwisowy kompatybilny z UPS Typ I – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Prąd wejściowy znamionowy	16 A;
Zasilanie sieciowe i wyjście UPS	IEC C20;
Wejście zasilania UPS	IEC C19;
Wyjście	1 x IEC C19, 6 x IEC C20;
Obudowa	Metalowa, rack, maksymalnie 1U z zestawem montażowym w szafie;
Czas transferu	Maksymalnie 5 ms.
Warunki gwarancji	2 lata;

	Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikat załączyć do oferty;** Oferowany przełącznik musi pochodzić z autoryzowanego kanału dystrybucji na rynek polski **– załączyć oświadczenie producenta**
Wymagania dodatkowe	Kaskadowanie, 4 x przewód zasilający, sygnalizacja stanu obejścia, klamry zabezpieczające gniazda IEC, przełącznik;

3. UPS - Typ II – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Rodzaj	Jedno – lub 3 fazowyazowy
Typ obudowy	Metalowa rack z zestawem montażwym w szafie rack;
Topologia	Podwójna konwersja online;
Czas transferu	0 ms.
Moc VA/W	10000/9000;
Układ przecieprzepięciowy	400J;
Ochrona przed przeciążeniem	125% przez 10 minut;
Czas pracy podtrzymania na baterii	10 minut przy pełnym obciążeniu/ 30 min. przy połowicznym – **załaczyć do oferty dokument potwierdzający autorstwa producenta urządzenia;**
Czas ładowania baterii	Maksymalnie 7h;
Złącza	1 x EPO, 1 x USB, RS-232, 2 x serial port, 2 x RJ45;
Rozpraszanie ciepła	Maksymalnie 2700 BTU/h
Hałas	Maksymalnie 60 dBA;
Warunki gwarancji	2 lata; Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikat załączyć do oferty;** Oferowany zasilacz musi pochodzić z autoryzowanego kanału dystrybucji na rynek polski **– załączyć oświadczenie producenta**
Wymagania dodatkowe	Kompatybilność z aktywnym PFC i generatorem, mozliwośc równoległego rozszerzenia do 4 jednostek, zdalne monitorowanie SNMP/HTTP, konfigurowalne napiecie i częstotliwość wyjściowa, panel LCD, wewnętrzny ogranicznik prądu, bezpiecznik, wewnętrzne automatyczne obejście, uruchamianie na baterii, wbudowany moduł zarządzania akumulatorem, filtrowanie EMI/RFI, kabel USB,;

4. Przełącznik serwisowy kompatybilny z UPS Typ II – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Prąd wejściowy znamionowy	60A;
Zasilanie sieciowe	Kostka zaciskowa;
Wejście zasilania UPS	Złącze AC;
Wyjście	Kostka zaciskowa, 4 x IEC C19, 4 x IEC C13;
Obudowa	Metalowa, rack, maksymalnie 2U z zestawem montażowym w szafie;
Czas transferu	Maksymalnie 0 ms.
Warunki gwarancji	2 lata;

	Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikat załączyć do oferty;** Oferowany przełącznik musi pochodzić z autoryzowanego kanału dystrybucji na rynek polski **– załączyć oświadczenie producenta**
Wymagania dodatkowe	Kaskadowanie, 2 x przewód zasilający;

5. Szafa rack – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	Szafa RACK 19" 24U 800x1000 mm, serwerowa, stojąca;
Chłodzenie	4 wenytylatory o średnicy 60 mm. każdy z termostatem o mocy 2,5 kW;
Materiał	Stal
Kolor	Szary lub czarny;
Nośność	1300 kg.;
Drzwi	Przednie preforowane, tylne perforowane dwuskrzydłowe, montaż lewo/prawo;
Ściany boczne	Zdejmowane, zamykane na zamek;
Szyney montazowe	4 szt.
Organizer kabli	2 x pionowy;
Klamka	Z zamkiem i 12 kluczami;
Waga	Maksymalnie 100 kg.
Certyfikaty	Potwierdzenie zgodności z normą PN-EN 62368-1:2015-03 **– załączyć do oferty;**
Wymagania dodatkowe	Złącze uziemiające, oznaczenia jednostek U na szynach rack, kólka i nóżki w zestawie, możliwość montażu cokołu, otwory na przewody wsuficie i podłodze, otwory wentylacyjne w suficie, podłodze i drzwiach, 4 otwory na wentylatory;

6. Koryto kablowe (kanał elektroinstalacyjny) Typ I – 15 szt.

1. Rozmiar - 40X60X2000;
2. Materiał: PVC
3. Wyposazenie: kanał, pokrywa, 4 klamry;
4. Palnośc: V1- V0;
5. Zgodnośc zdyrektywą RoHS;
6. Deklaracje CE, deklaracja SEP-BBJ – **załączyć do oferty;**

7. Koryto kablowe (kanał elektroinstalacyjny) Typ II – 10 szt.

1. Rozmiar - 15X17X2000;
2. Materiał: PVC
3. Wyposazenie: kanał, pokrywa;
4. Palnośc: V1- V0;
5. Zgodnośc zdyrektywą RoHS;
6. Deklaracje CE, deklaracja SEP-BBJ – **załączyć do oferty;**

8. Przewód Typ I – 30 mb.

1. Dopuszczalna temperatura otoczenia kabla po montażu (bez wibracji):-40 do 50 stopni Celsjusza
2. Dopuszczalna temperatura otoczenia kabla podczas montażu:-25 do 50 stopni Celsjusza
3. Gatunek materiału izolacji żyły:Guma etylenowo-propylenowa (EPR)
4. Gatunek materiału powłoki zewnętrznej: Guma (CPE/CSP)
5. Identyfikacja żył: Kolor
6. Klasa reakcji na ogień wg EN 13501-6: Eca
7. Klasa żyły: 5 = wielodrutowa giętka
8. Liczba żył: 5
9. Maksymalna temperatura żyły: 60 °C
10. Materiał izolacji żyły: Guma
11. Model/kształt/forma: Okrągły
12. Napięcie znamionowe U: 750 V
13. Napięcie znamionowe U0: 450 V
14. Nierozprzestrzeniający płomienia: Zgodnie z EN 60332-1-2
15. Odporność na niską temperaturę zgodnie z EN 60811-504+505+506;
16. Olejoodporność zgodnie z EN 60811-2-1;
17. Olejoodporność zgodnie z EN 60811-404;
18. Znamionowy przekrój żyły:16
19. Żyła ochronna;
20. Deklaracja zgodności – **załaczyć do oferty;**

9. Przewód Typ II – 30 mb.

1. Klasa żyły: 5 = giętki
2. Model: Okrągły
3. Identyfikacja żył: Kolor
4. Dopuszczalna temperatura kabla dla połączeń ruchomych [°C] – maksymalnie 55
5. Dopuszczalna temperatura kabla ułożonego na stałe [°C] – maksymalnie 75
6. Liczba żył: 3
7. Napięcie znamionowe U [V]: 750
8. Znamionowy przekrój żyły [mm2]: 16
9. Izolacja żyły: Guma (EPR)
10. Materiał powłoki zewnętrznej: Guma (EPR)
11. Żyła ochronna
12. Dopuszczalna temperatura kabla dla połączeń ruchomych [°C]:-25
13. Dopuszczalna temperatura kabla ułożonego na stałe [°C]: -25
14. Napięcie znamionowe U0 [V]: 450
15. Maksymalna temperatura żyły [°C]: 60

10. Wyłącznik nadprądowy Typ I – 1 szt.

1. Liczba biegunów chronionych – 3
2. Układ biegunów - 3 P
3. Charakterystyka wyzwalania – C
4. Liczba modułów – 3

5. Znamionowa zwarciowa zdolność łączeniowa Icn - 6 kA
6. Napięcie znamionowe łączeniowe Ue (AC) - 230 / 400 V
7. Typ napięcia zasilającego – AC
8. Częstotliwość - 50/60
9. Znamionowe napięcie izolacji Ui - 500 V
10. Znamionowe napięcie udarowe wytrzymywane Uimp - 4000 V
11. Prąd znamionowy In - 32 A
12. Prąd znamionowy wyłączalny zwarciowy roboczy Ics - 6 kA
13. Min./max. wartość natężenia prądu AC zadziałania zabezpieczenia bezzwłocznego - 5 / 10 In
14. Min./max. wartość natężenia prądu DC zadziałania zabezpieczenia bezzwłocznego - 7 / 15 In
15. Min./max. wartość natężenia prądu DC zadziałania zabezpieczenia zwłocznego - 1.13 / 1.45 In
16. Zdolność wyłączania 1P przy 400 V (EN 60947-2) - 3 kA
17. Znam. zdolność wyłącz. zwarciowego Icn poniżej 400V AC zgodnie z IEC 60898-1 - 6 kA
18. Zdolność wyłączania 400V (NF EN 60947-2) - 10 kA
19. Zdolność wyłączania 415V (NF EN 60947-2) - 10 kA
20. Prąd znamionowy w temperaturze -25°C - 39.9 A
21. Prąd znamionowy w temperaturze 0°C - 36.5 A
22. Prąd znamionowy w temperaturze 25°C - 32.8 A
23. Współczynnik korekcyjny prądu znam. dla 3 aparatów zainstalowanych obok siebie - 0.95
24. Współczynnik korekcyjny wyzwalacza bezzwłocznego przy czestotliwości 100 Hz - 1.1
25. Współczynnik korekcyjny wyzwalacza bezzwłocznego przy czestotliwości 200 Hz - 1.2
26. Współczynnik korekcyjny wyzwalacza bezzwłocznego przy czestotliwości 400 Hz - 1.5
27. Częstotliwość (zakres do ETIM) - 50 do 60 Hz
28. Całkowite straty mocy dla prądu znamionowego - 13 W
29. Straty mocy na biegun dla prądu znamionowego - 4.9 W
30. Wytrzymałość elektryczna (liczba cykli) – 4000
31. Wytrzymałość mechaniczna (liczba cykli) – 20000
32. Zgpdnośc z normą EN 60898-1
33. Stopień ochrony - IP20
34. Stopień zanieczyszczenia zgodnie z IEC 60664 / IEC 60947-2 – 2
35. Klasa ograniczenia energii I^2t. - 3

11. Wyłącznik różnicowoprądowy Typ I – 1 szt.

1. Liczba biegunów - 2 P
2. Montaż - szyna DIN
3. Liczba modułów – 2
4. Napięcie znamionowe łączeniowe Ue (AC) - 230 V
5. Częstotliwość – 50 Hz;
6. Znamionowe napięcie izolacji Ui - 500 V
7. Znamionowe napięcie udarowe wytrzymywane Uimp - 4000 V
8. Znamionowy prąd różnicowy dI - 30 m
9. Prąd znamionowy In - 63 A
10. Znamionowy prad wyładowczy (In 8/20µs) - 0.25 kA
11. Znamionowa zdolność załączania i wyłączania Im - 1.5 kA
12. Znamionowy warunkowy prąd zwarciowy Inc zgodnie z PN-EN 61008-1 - 6 kA
13. Prąd znamionowy w temperaturze -25°C - 63 A
14. Prąd znamionowy w temperaturze 0°C - 63 A
15. Prąd znamionowy w temperaturze 25°C - 63 A
16. Wytrzymałość elektryczna (liczba cykli) – 2000

17. Wytrzymałość mechaniczna (liczba cykli) – 4000
18. Moment dokręcający - 2,8 Nm
19. Pojemność zacisku wyjściowego dla przewodu sztywnego (drut) - 1 / 25 mm²
20. Zgodnośc znormą EN 61008-1
21. Stopień ochrony - IP20
22. Typ wyłącznika różnicowoprądowego – A;

12. Wyłącznik różnicowoprądowy Typ II – 1 szt.

1. Liczba biegunów - 2 P
2. Montaż - Szyna DIN
3. Liczba modułów – 2
4. Napięcie znamionowe łączeniowe Ue (AC) - 230 V
5. Znamionowe napięcie izolacji Ui - 500 V
6. Znamionowe napięcie udarowe wytrzymywane Uimp - 4000 V
7. Znamionowy prąd różnicowy dI - 30 mA
8. Prąd znamionowy In - 25 A
9. Znamionowy prad wyładowczy (In 8/20µs) - 0.25 kA
10. Znamionowa zdolność załączania i wyłączania Im - 1.5 kA
11. Znamionowy warunkowy prąd zwarciowy Inc zgodnie z PN-EN 61008-1 - 6 kA
12. Prąd znamionowy w temperaturze -25°C - 25 A
13. Prąd znamionowy w temperaturze 0°C - 25 A
14. Prąd znamionowy w temperaturze 25°C - 25 A
15. Częstotliwość (zakres do ETIM) - 50 H
16. Całkowite straty mocy dla prądu znamionowego - 2.32 W
17. Straty mocy na biegun dla prądu znamionowego – 1,23 W
18. Wytrzymałość elektryczna (liczba cykli) – 2000
19. Wytrzymałość mechaniczna (liczba cykli) – 4000
20. Moment dokręcający - 2,8 Nm
21. Pojemność zacisku wyjściowego dla przewodu sztywnego (drut) - 1 / 25 mm²
22. Rodzaj przyłącza - ze śrubą
23. Zgodność z normą EN 61008-1
24. Stopień ochrony - IP20
25. Typ wyłącznika różnicowoprądowego – A
26. Stopień zanieczyszczenia zgodnie z IEC 60664 / IEC 60947-2 - 2

13. Wyłącznik nadprądowy Typ II – 2 szt.

1. Liczba biegunów chronionych – 1
2. Liczba biegunów - 1 P
3. Układ biegunów - 1 P
4. Charakterystyka wyzwalania – C
5. Liczba modułów – 1
6. Znamionowa zwarciowa zdolność łączeniowa Icn - 6 kA
7. Napięcie znamionowe łączeniowe Ue (AC) - 230 / 400 V
8. Typ napięcia zasilającego – AC
9. Znamionowe napięcie izolacji Ui - 500 V
10. Znamionowe napięcie udarowe wytrzymywane Uimp - 4000 V
11. Prąd znamionowy In - 16 A
12. Prąd znamionowy wyłączalny zwarciowy roboczy Ics - 6 kA

13. Znam. zdolność wyłącz. zwarciowego Icn poniżej 230V AC zgodnie z IEC 60898-1 - 6 kA
14. Prąd znamionowy wyłączalny zwarciowy graniczny Icu dla ETIM (PN-EN 60947-2) - 6 kA
15. Prąd znamionowy w temperaturze -25°C - 22.48 A
16. Prąd znamionowy w temperaturze 0°C - 19.61 A
17. Prąd znamionowy w temperaturze 25°C - 16.75 A
18. Współczynnik korekcyjny prądu znam. dla 2 aparatów zainstalowanych obok siebie – 1
19. Współczynnik korekcyjny wyzwalacza bezzwłocznego przy czestotliwości 100 Hz - 1.1
20. Współczynnik korekcyjny wyzwalacza bezzwłocznego przy czestotliwości 200 Hz - 1.2
21. Współczynnik korekcyjny wyzwalacza bezzwłocznego przy czestotliwości 400 Hz - 1.5
22. Częstotliwość (zakres do ETIM) - 50 do 60 Hz
23. Całkowite straty mocy dla prądu znamionowego - 2.32 W
24. Straty mocy na biegun dla prądu znamionowego - 2.32 W
25. Wytrzymałość elektryczna (liczba cykli) – 4000
26. Wytrzymałość mechaniczna (liczba cykli) – 20000
27. Moment dokręcający - 2,8 Nm
28. Przekrój przewodu elastycznego (linka) w zacisku - 1 / 25mm²
29. Zgodnośc znormą EN 60898-1
30. Stopień ochrony - IP20
31. Stopień zanieczyszczenia zgodnie z IEC 60664 / IEC 60947-2. – 2
32. Klasa ograniczenia energii I^2t. – 3

14. Wyłącznik nadprądowy Typ III – 2 szt.

1. Liczba biegunów chronionych – 1
2. Liczba biegunów - 1 P
3. Układ biegunów - 1 P
4. Charakterystyka wyzwalania – C
5. Liczba modułów – 1
6. Znamionowa zwarciowa zdolność łączeniowa Icn - 6 kA
7. Napięcie znamionowe łączeniowe Ue (AC) - 230 / 400 V\
8. Typ napięcia zasilającego – AC
9. Znamionowe napięcie izolacji Ui - 500 V
10. Znamionowe napięcie udarowe wytrzymywane Uimp - 4000 V
11. Prąd znamionowy In - 32 A
12. Prąd znamionowy wyłączalny zwarciowy roboczy Ics - 6 kA
13. Znam. zdolność wyłącz. zwarciowego Icn poniżej 230V AC zgodnie z IEC 60898-1 - 6 kA
14. Prąd znamionowy wyłączalny zwarciowy graniczny Icu dla ETIM (PN-EN 60947-2) - 10 kA
15. Zdolność wyłączania 240V (NF EN 60947-2) - 10 kA
16. Prąd znamionowy w temperaturze -25°C - 41.8 A
17. Prąd znamionowy w temperaturze 0°C - 37.7 A
18. Prąd znamionowy w temperaturze 25°C - 33.6 A
19. Współczynnik korekcyjny prądu znam. dla 2 aparatów zainstalowanych obok siebie – 1
20. Współczynnik korekcyjny wyzwalacza bezzwłocznego przy czestotliwości 100 Hz - 1.1;
21. Współczynnik korekcyjny wyzwalacza bezzwłocznego przy czestotliwości 200 Hz - 1.2;
22. Współczynnik korekcyjny wyzwalacza bezzwłocznego przy czestotliwości 400 Hz - 1.5;
23. Częstotliwość (zakres do ETIM) - 50 do 60 Hz
24. Całkowite straty mocy dla prądu znamionowego - 4.4 W
25. Straty mocy na biegun dla prądu znamionowego - 4.4 W
26. Wytrzymałość elektryczna (liczba cykli) – 4000
27. Wytrzymałość mechaniczna (liczba cykli) – 20000

28. Moment dokręcający - 2,8 Nm
29. Rodzaj przyłącza - ze śrubą
30. Zgodność z normą EN 60898-1
31. Stopień ochrony - IP20;

15. Szyna grzebieniowa – 1 szt.

1. Liczba biegunów - 1 P
2. Dostosowana do współpracy z urządzeniami modularnymi;
3. Napięcie znamionowe łączeniowe Ue (AC) - 415 V
4. Napięcie pracy - 230 V
5. Prąd znamionowy In - 80 A
6. Długość - 210 mm
7. Przekrój przewodu sztywnego (drut) w zacisku - 16mm²
8. Rodzaj przyłącza - ze śrubą;
9. Liczba urządzeń możliwych do wbudowania – 12
10. Izolowana;

16. Rozłącznik izolacyjny – 1 szt.

1. Liczba biegunów - 4 P
2. Układ biegunów - 4 P
3. Liczba modułów – 4
4. Napięcie znamionowe łączeniowe Ue (AC) - 400 V
5. Znamionowe napięcie izolacji Ui - 440 V
6. Rodzaj wejścia napięcia – AC
7. Znamionowe napięcie udarowe wytrzymywane Uimp - 6000
8. Obciążalność prądowa prądu przemiennego AC21 w kategorii B - 63 A
9. Dopuszczalne obciążenie prądem AC22 kategorii A - 63 A
10. Prąd znamionowy In - 63
11. Znamionowy krótkotrwały prąd wytrzymywany 1s - 0.945 kA
12. Obudowa zewnętrzna zasilana prądem cieplnym - 63 A
13. Częstotliwość (zakres do ETIM) - 50 do 60 Hz
14. Całkowite straty mocy dla prądu znamionowego - 9.2 W
15. Straty mocy na biegun dla prądu znamionowego 2.3 W
16. Trwałość elektryczna przy obciążeniu nominalnym w cyklach roboczych (AC21) – 5000
17. Trwałość elektryczna przy obciążeniu nominalnym w cyklach roboczych (AC22) – 5000
18. Wytrzymałość mechaniczna (liczba cykli) – 60000
19. Moment dokręcający - 2,8 Nm
20. Przekrój przewodu elastycznego (linka) w zacisku - 2,5 / 16mm²
21. Przekrój przewodu sztywnego (drut) w zacisku - 2,5 / 25mm²
22. Rodzaj przyłącza - ze śrubą
23. Liczba styków NO – 4
24. Zgodność z normą IEC 60947-3,IEC/EN 60669-2,IEC/EN 60669-4
25. Stopień ochrony - IP20
26. Stopień zanieczyszczenia zgodnie z IEC 60664 / IEC 60947-2 – 2;

17. Rozdzielnica naścienna – 1 szt.

1. Zgodność z normą: PN-EN 60439-

2. Stopień ochrony: IP40
3. II klasa ochronności
4. Kolor biały RAL 9010, drzwi przeźroczyste;
5. Wyposażona w listwy przyłączeniowe N+P
6. Pokrywa mocowana za pomocą wkrętów izolacyjnyc
7. Liczba rzędów: 3
8. 36 modułów 17,5 mm w rzędzie;
9. Odporność na żar – 650 stopni Celsjusza;

18. Przycisk przeciwpożarowy – 1 szt.

1. Ręczny ostrzegacz pożarowy OP1 przeznaczony jest do stosowania w pomieszczeniach przemysłowych użytku publicznego
2. Nadtynkowy;
3. 1 łącznik zwiernym i 1 rozwierny;
4. Po zbiciu szybki przycisk musi zostać zwolniony samoczynnie (typ A wg PN-EN 54-11)
5. Możliwośc instalacji 3 łączników zwiernych lub rozwiernych;
6. Mozliwośc instalacji diody, którą można podłączyć do łącznika lub bezpośrednio do instalacji alarmowej obiektu;
7. Uruchomienie i wysłanie sygnału następuje przez zbicie szybki;
8. Kasowanie stanu alarmowego następuje przez wymianę szybki;
9. Wyrób musi być zgodny z normą PN-EN 54-11.
10. Kolor produktu – czerwony
11. Samoczynne zwolnienie przycisku)
12. Prąd znamionowy ciągły: 10A
13. Rodzaj zestyku: NO (styk zwierny), NC (styk rozwierny);
14. Znamionowe napięcie izolacji: 500 V
15. Prąd znamionowy łączeniowy: 2,5 A (230 V AC), 1,6 A (400/500 V AC), 4 A (24 V DC), 1 A (110 V DC), 0,25 A (220 V DC);
16. Przekrój przewodów podłączeniowych: 2× 1 do 2,5 mm² (jednodrutowych) i 2 x × 0,75 do 1,5 mm² (linek)
17. Stopień ochrony: IP65;
18. Ochrona prze wodą zgodnie z normą PN-EN60068-2-30;

19. Przewód Typ III – 20 mb.

1. Bezhalogenowy zgodnie z normą EN 50267-2-2;
2. Dopuszczalna temperatura otoczenia kabla po montażu (bez wibracji): - 90 °C
3. Dopuszczalna temperatura otoczenia kabla podczas montażu - 90 °C
4. Identyfikacja żył - Kolor
5. Klasa żyły - 1 = jednodrutowy
6. Liczba żył - 2;
7. Materiał izolacji żyły - guma (EPR)
8. Napięcie znamionowe U - 1000 kV
9. Napięcie znamionowe U0 - 600 kV
10. Nierozprzestrzeniający płomienia - zgodnie z EN 60332-1-2
11. Niska emisja dymów zgodnie z EN 61034-2;
12. Średnica zewnętrzna - 7.5 mm
13. Znamionowy przekrój żyły - 1.5

20. Wykonawca dokona instalacji i konfiguracji urządzeń wymienionych powyżej w pkt. VI, w tym co najmniej:

1. Przygotowanie trasy kablowej serwerownia-rozdzielnica główna;
2. Montaż okablowania zasilającego urządzeń UPS i przełączników serwisowych;
3. Przygotowanie trasy kablowej serwerownia-przycisk przeciwpożarowy;
4. Montaż okablowania przycisku przeciwpożarowego I samego przycisku;
5. Przygotowanie miejsca pod szafę stojącą RACK w serwerowni
6. Montaż szafy RACK i ustawienie jej w docelowym miejscu
7. Montaż urządzeń UPS i przełączników serwisowych wraz ze wszystkimi niezbędnymi akcesoriami w szafie RACK
8. Podłączenie okablowania pod urządzenia UPS i przełączniki serwisowe zgodnie z wytycznymi producenta
9. Montaż zabezpieczeń dla urządzeń UPS i przełączników serwisowych w rozdzielnicy głównej budynku
10. Podpięcie urządzeń UPS i przełączników serwisowych do zasilania zgodnie z wytycznymi producenta
11. Podpięcie odbiorów (główna szafa RACK i rozdzielnica komputerowa) pod dedykowane zaciski na przełącznikach serwisowych;
12. Uruchomienie systemu;
13. Testy sytemu (sprawdzenie poprawności przełączania sprawdzenie działania wszystkich urządzeń wchodzących w skład systemu

VII. Stacja robocza Typ I – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	Komputer stacjonarny.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej
Wydajność	Oferowany komputer musi osiągać w teście wydajności SYSMARK 25 Overall Rating, wynik 1400 pkt. **Wydruk z oprogramowania testującego 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	8 GB DDR4. Możliwość rozbudowy do 32 GB;
Pamięć masowa	SSD 512 GB;

	Możliwość instalacji dodatkowego dysku twardego M.2 lub 2.5	
Grafika	Zintegrowana z procesorem musi umożliwiać pracę dwumonitorową; Karta osiągająca w teście PC Mark 10 Digital Content Creation wynik 4000 punktów – **wydruk zoprogramowania testującego załączyć do oferty.**	
Matryca	Rozmiar matrycy / plamki	23,8” / maksymalnie. 0,275mm
	Rozdzielczość	FHD (1920x1080)
	Jasność typowa	250 cd/m²
	Kontrast typowy	600:1
	Kąty Horizontal/Vertical	178/ 178 stopni
	Rodzaj matrycy	Matowa IPS
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 0,9 MP z diodą LED informującą użytkownika o pracy, Mechaniczna przesłona kamery w obudowie (nie dopuszcza się kamer przekręcanych). Wbudowane w obudowę dwa mikrofony	
Obudowa	Typu All-in-One zintegrowana z monitorem 23.8 cali. Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Zasilacz o mocy 65W o efektywności 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności 82% przy obciążeniu zasilacza na poziomie 100%, Wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS. Podstawa jednostki musi umożliwiać regulację pochyłu pionowego w zakresie od -5 do 20 stopni.	
Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową, a także zapewniająca monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej oraz zdalną konfigurację ustawień BIOS	
Bezpieczeństwo	Płyta główna zawierająca 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 Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi zachowywać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego.	

BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy. Przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury. Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego. Możliwość, ustawienia hasła na poziomie: - administratora [hasło nadrzędne] - użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywanie zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego]. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość wyłączenia/włączenia karty sieciowej Możliwość włączenia/wyłączenia kontrolera SATA Możliwość włączenia/wyłączenia kontrolera audio, Możliwość włączenia/wyłączenia układu TPM. Możliwość włączenia/wyłączenia wbudowanej kamery i czytnika kart multimedialnych Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. Możliwość zdefiniowania automatycznego uruchamiania komputera w dwóch trybach: codziennie lub w wybrane dni tygodnia, Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacja. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.
Certyfikaty i standardy	Komputer musi być wyprodukowany zgodnie z normami ISO9001, ISO45001 i ISO50001 – **certyfikaty załączyć do oferty;**
Wbudowane porty	1x HDMI 1x USB 3.2 Typ-C 3x USB 3.2 Typ-A Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub’ów. Wszystkie porty dostępne dla użytkownika w najniższej możliwej regulacji wysokości 1x Universal audio jack

	1x RJ-45 port 10/100/1000 Mbps Karta WiFi ax+ bluetooth 5.1 Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki; wyposażona w 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, 1 złącze M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi. Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)
Warunki gwarancji i serwisu	3-letnia gwarancja producenta; Czas reakcji serwisu, do końca następnego dnia roboczego. Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikat załączyć do oferty**
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w języku polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 9. Graficzne środowisko instalacji i konfiguracji w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 16. Konta i profile użytkowników zarządzane zdalnie; 17. Praca systemu w trybie ochrony kont użytkowników. 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 19. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".

	20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 28. Wbudowany mechanizm wirtualizacji typu hypervisor; 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 40. Możliwość tworzenia wirtualnych kart inteligentnych. 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 42. Wsparcie dla IPSEC oparte na politykach; 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 44. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 45. Umozliwiajacy pracę w domenie;

Oprogramowanie użytkowe	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + musi umożliwiać co najmniej: 1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu, 6. Automatyczne odłączanie zainfekowanej końcówki od sieci, 7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. 8. Zarządzanie stacją kliencką poprzez zbieranie informacji co najmniej o: nazwie, 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 (procesor, RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach. 9. Musi posiadać moduł ochrony IDS/IPS 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie do szyfrowania, chroniące dane na stacji za pomocą algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Pełne szyfrowanie dysków działających w oferowanych komputerach zapobiegające utracie danych z powodu utraty / kradzieży stacji roboczej. 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępniać ją tylko autoryzowanym użytkownikom. 16. Musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji; 17. Musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji. 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 19. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 20. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko do procesów systemowych oraz zaufanych aplikacji. 21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika.

	22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych ochroną any ransomware. 23. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware; 24. Centralna konsola zarządzająca umożliwiająca co najmniej: a) przechowywanie danych w bazie typu SQ b) zdalną instalację lub deinstalację oprogramowania, na pojedynczych stacjach, zakresie adresów IP lub grupie z ActiveDirectory; c) tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi oraz formatach dla systemów Linux d) centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik na serwerz konsoli; e) raportowanie z prezentacją tabelaryczną i graficzną, możliwością automatycznego czyszczenia starych raportów, eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich; f) definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; g) Możliwość tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera; h) Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach; i) Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń j) 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. k) Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 25. System musi umożliwiać, z konsoli na serwerze, co najmniej: 26. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie 27. przyznawanie praw dostępu dla nośników pamięci tj. USB, CD 28. regulowania połączeń WiFi i Bluetooth 29. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe 30. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi 31. blokowanie dostępu dowolnemu urządzeniu 32. tymczasowe dodanie dostępu do urządzenia przez administratora 33. szyfrowanie zawartości USB i udostępnianie jej na stacjach końcowych; 34. zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszk 35. zezwalanić na dostęp tylko urządzeniom wcześniej dodanym przez administratora 36. używanda tylko zaufanych urządzeń sieciowych;

	37. Funkcja wirtualnej klawiatury 38. Możliwość blokowania każdej aplikacji , w tym w oparciu o kategorie 39. Możliwość dodania własnych aplikacji do listy zablokowanych 40. Tworzenie listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze 41. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 42. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki; 43. Możliwość zablokowania funkcji Printscreen 44. Monitorowanie przesyłu danych między aplikacjami; 45. Monitorowanie i kontrola przepływu poufnych informacji 46. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj 47. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe; 48. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 49. Ochrona zawartości schowka systemu 50. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 51. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych 52. Ochrona plików zamkniętych w archiwach 53. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 54. Możliwość tworzenia profilu DLP dla każdej polityki 55. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 56. Ochrona przez wyciekiem plików poprzez programy typu p2p 57. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 58. Monitorowanie określonych rodzajów plików. 59. Możliwość wykluczenia określonych plików/folderów z procedury monitorowania. 60. Możliwość śledzenia zmian we wszystkich plikach 61. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na stacjach roboczych; 62. Możliwość definiowana własnych typów plików 63. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku 64. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem 65. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 66. System ochrony i zarządzania urządzeniami za pomocą platformy w chmurze;. 67. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 68. Musi posiadać możliwość eksportu danych użytkownika 69. Import listy urządzeń z pliku CSV 70. Dodawanie urządzeń;

	71. Podgląd co najmniej następujących informacji konfiguracji: data i status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta 72. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, wolna przestrzeń na dysku, całkowita przeszłość na dysku, użycie procesora,; 73. Podgląd zainstalowanych aplikacji; 74. Moduł raportowania aktywności, skanowania oraz naruszenia reguł; 75. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa dostępne przez przeglądarkę internetową; 76. Portal zarządzający w postaci SaaS; 77. Skanowanie podatności za pomocą nodów skanujących; 78. Nody skanujące w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 79. Portal zarządzający musi umożliwiać: 80. przegląd wybranych danych; 81. zablokowanie możliwości zmiany konfiguracji; 82. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów; 83. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności 84. eksport skanów podatności do pliku CSV; 85. **D**eduplikacja danych na źródle, 86. Backup przyrostowy i różnicowy, 87. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 88. Backup danych lokalnych – plikowy oraz poczty; 89. Backup otwartych plików; 90. Filtr plików oraz folderów, 91. Domyślne wykluczenia zbędnych plików 92. Przywracanie danych do wskazanej lokalizacji, 93. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, 94. Wyszukiwanie plików w repozytorium użytkownika, 95. Automatyczne logowanie, 96. Zapamiętywanie danych logowania, 97. Automatyczne uruchamianie programu przy starcie systemu, 98. Ustawianie priorytetu dla procesu backupu, 99. Zmiana klucza szyfrującego, 100. Konfiguracja wydajności procesu backupu, 101. Zastępowanie nazwy pliku GUID-em, 102. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, 103. Kompresja danych, 104. Transmisja po bezpiecznym protokole TLS, 105. Deklaracja klucza szyfrującego dane użytkownika, 106. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 107. Obliczanie sumy kontrolnej, 108. Kopie zapasowe musza być przechowywane w data center, na terenie Polski. 109. Licencje muszą być przypisywane do urządzenia z limitem pojemności przestrzeni w chmurze minimum 50 GB;

	110. Wsparcie techniczne, świadczone w języku polskim; 111. Zarządzanie, monitoring, konfigurację oraz dystrybucję ustawień BIOS; 112. Oprogramowanie produkowane przez producenta komputera z nieograniczoną czasowo licencją umożliwiającą: 113. Upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji; 114. Mozliwość sprawdzenia każdego sterownika, aplikacji, BIOS'u bezpośrednio na stronie producenta przed instalacją oraz uzyskanie informacji o: a. poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodności z systemami operacyjnymi 115. Uzyskanie wylazu najnowszych aktualizacji z podziałem na krytyczne, rekomendowane i opcjonalne 116. Włączenie/wyłączenie funkcji automatycznego restartu; 117. Rozpoznanie modelu oferowanego komputera, numeru seryjnego, uzyskanie informacj kiedy dokonany został ostatnio upgrade; 118. Sprawdzenie historii upgrade'ów z informacją jakie sterowniki były instalowane; 119. Uzyskanie wykazu wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji; 120. Uzyskanie raportu uwzględniającego informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach

VIII. Stacja robocza Typ II – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	Komputer stacjonarny.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej
Wydajność	Oferowany komputer musi osiągać w teście wydajności SYSMARK 25 Overall Rating, wynik 1500 pkt. **Wydruk z oprogramowania testującego 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	16 GB DDR4. Możliwość rozbudowy do 64 GB;	
Pamięć masowa	512GB SSD M.2 NVMe Możliwość instalacji dodatkowego dysku twardego M.2 lub 2.5	
Grafika	Zintegrowana z procesorem musi umożliwiać pracę dwumonitorową; Karta osiągająca w teście PC Mark 10 Digital Content Creation wynik 4000 punktów – **wydruk z oprogramowania testującego załączyć do oferty.**	
Matryca	Rozmiar matrycy	27”
	Rozdzielczość	FHD (1920x1080)
	Jasność typowa	250 cd/m²
	Kontrast typowy	700:1
	Kąty Horizontal/Vertical	178/ 178 stopni
	Rodzaj matrycy	Matowa IPS
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 5.0 MP z diodą LED informującą użytkownika o pracy, Mechaniczna przesłona kamery w obudowie (nie dopuszcza się kamer przekręcanych). Wbudowane w obudowę dwa mikrofony	
Obudowa	Typu All-in-One zintegrowana z monitorem 27 cali. Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki); Musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA; Zasilacz o mocy 130W o efektywności 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności 82% przy obciążeniu zasilacza na poziomie 100%, Wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System diagnostyczny musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS. Podstawa jednostki musi umożliwiać regulację pochyłu pionowego w zakresie od -5 do 20 stopni, regulację wysokości w zakresie 10 cm oraz obrót ekranu (PIVOT).	
Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową IPv4 oraz w oparciu o protokół IPv6, a także zapewniająca: - Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; - Zdalną konfigurację ustawień BIOS; - Zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;	

	- Zapis i przechowywanie informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów) z wbudowanej pamięci nieulotnej. - Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym musi być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/);
Bezpieczeństwo	Płyta główna zawierająca 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 Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot'owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi zachowywać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego. Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy. Przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury. Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego. Możliwość, ustawienia hasła na poziomie: - administratora [hasło nadrzędne] - użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywanie zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego]. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość wyłączenia/włączenia karty sieciowej Możliwość włączenia/wyłączenia układu TPM. Możliwość włączenia/wyłączenia wbudowanej kamery i czytnika kart multimedialnych Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacji. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.
Certyfikaty i standardy	Komputer musi być wyprodukowany zgodnie z normami ISO9001, ISO45001 i ISO50001 – **certyfikaty załączyć do oferty;** Certyfikat TCO - **do oferty załączyć certyfikat lub wydruk ze strony http://tcocertified.com/product-finder/**

Wbudowane porty	1x HDMI 1x DisplayPort 1x USB 3.2 Typ-C 4x USB 3.2 Typ-A 2x USB 2.0 Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub'ów itp. Wszystkie porty dostępne dla użytkownika w najniższej możliwej regulacji wysokości 1x Universal audio jack 1x One Line-out audio 1x RJ-45 port 10/100/1000 Mbps 1x Czytnik kart SD Karta WiFi ax+ bluetooth 5.2 Nagrywarka DVDRW wbudowana w obudowę komputera; Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, wyposażona w 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, 1 złącze M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi, slot PCIe x16 Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)
Warunki gwarancji i serwisu	3-letnia gwarancja producenta; Czas reakcji serwisu, do końca następnego dnia roboczego. Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikat załączyć do oferty**
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w języku polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 9. Graficzne środowisko instalacji i konfiguracji w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego.

	13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 16. Konta i profile użytkowników zarządzane zdalnie; 17. Praca systemu w trybie ochrony kont użytkowników. 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 19. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 28. Wbudowany mechanizm wirtualizacji typu hypervisor; 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM

	39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 40. Możliwość tworzenia wirtualnych kart inteligentnych. 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 42. Wsparcie dla IPSEC oparte na politykach; 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 44. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 45. Umozliwiajacy pracę w domenie;
Oprogramowanie użytkowe	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + musi umożliwiać co najmniej: 1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu, 6. Automatyczne odłączanie zainfekowanej końcówki od sieci, 7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. 8. Zarządzanie stacją kliencką poprzez zbieranie informacji co najmniej o: nazwie, 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 (procesor, RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach. 9. Musi posiadać moduł ochrony IDS/IPS 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie do szyfrowania, chroniące dane na stacji za pomocą algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Pełne szyfrowanie dysków działających w oferowanych komputerach zapobiegające utracie danych z powodu utraty / kradzieży stacji roboczej. 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępniać ją tylko autoryzowanym użytkownikom. 16. Musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji; 17. Musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji.

	18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 19. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 20. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko do procesów systemowych oraz zaufanych aplikacji. 21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych ochroną any ransomware. 23. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware; 24. Centralna konsola zarządzająca umożliwiająca co najmniej: a) przechowywanie danych w bazie typu SQ b) zdalną instalację lub deinstalację oprogramowania, na pojedynczych stacjach, zakresie adresów IP lub grupie z ActiveDirectory; c) tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi oraz formatach dla systemów Linux d) centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik na serwerz konsoli; e) raportowanie z prezentacją tabelaryczną i graficzną, możliwością automatycznego czyszczenia starych raportów, eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich; f) definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; g) Możliwość tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera; h) Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach; i) Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń j) 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. k) Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 25. System musi umożliwiać, z konsoli na serwerze, co najmniej: 26. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie 27. przyznawanie praw dostępu dla nośników pamięci tj. USB, CD

	28. regulowania połączeń WiFi i Bluetooth 29. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe 30. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi 31. blokowanie dostępu dowolnemu urządzeniu 32. tymczasowe dodanie dostępu do urządzenia przez administratora 33. szyfrowanie zawartości USB i udostępnianie jej na stacjach końcowych; 34. zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszk 35. zezwalanić na dostęp tylko urządzeniom wcześniej dodanym przez administratora 36. używanda tylko zaufanych urządzeń sieciowych; 37. Funkcja wirtualnej klawiatury 38. Możliwość blokowania każdej aplikacji , w tym w oparciu o kategorie 39. Możliwość dodania własnych aplikacji do listy zablokowanych 40. Tworzenie listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze 41. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 42. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki; 43. Możliwość zablokowania funkcji Printscreen 44. Monitorowanie przesyłu danych między aplikacjami; 45. Monitorowanie i kontrola przepływu poufnych informacji 46. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj 47. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe; 48. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 49. Ochrona zawartości schowka systemu 50. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 51. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych 52. Ochrona plików zamkniętych w archiwach 53. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 54. Możliwość tworzenia profilu DLP dla każdej polityki 55. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 56. Ochrona przez wyciekiem plików poprzez programy typu p2p 57. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 58. Monitorowanie określonych rodzajów plików. 59. Możliwość wykluczenia określonych plików/folderów z procedury monitorowania. 60. Możliwość śledzenia zmian we wszystkich plikach 61. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na stacjach roboczych; 62. Możliwość definiowana własnych typów plików 63. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku

	64. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem 65. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 66. System ochrony i zarządzania urządzeniami za pomocą platformy w chmurze;. 67. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 68. Musi posiadać możliwość eksportu danych użytkownika 69. Import listy urządzeń z pliku CSV 70. Dodawanie urządzeń; 71. Podgląd co najmniej następujących informacji konfiguracji: data i status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta 72. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, wolna przestrzeń na dysku, całkowita przeszłość na dysku, użycie procesora,; 73. Podgląd zainstalowanych aplikacji; 74. Moduł raportowania aktywności, skanowania oraz naruszenia reguł; 75. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa dostępne przez przeglądarkę internetową; 76. Portal zarządzający w postaci SaaS; 77. Skanowanie podatności za pomocą nodów skanujących; 78. Nody skanujące w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 79. Portal zarządzający musi umożliwiać: 80. przegląd wybranych danych; 81. zablokowanie możliwości zmiany konfiguracji; 82. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów; 83. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności 84. eksport skanów podatności do pliku CSV; 85. **D**eduplikacja danych na źródle, 86. Backup przyrostowy i różnicowy, 87. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 88. Backup danych lokalnych – plikowy oraz poczty; 89. Backup otwartych plików; 90. Filtr plików oraz folderów, 91. Domyślne wykluczenia zbędnych plików 92. Przywracanie danych do wskazanej lokalizacji, 93. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, 94. Wyszukiwanie plików w repozytorium użytkownika, 95. Automatyczne logowanie, 96. Zapamiętywanie danych logowania, 97. Automatyczne uruchamianie programu przy starcie systemu, 98. Ustawianie priorytetu dla procesu backupu, 99. Zmiana klucza szyfrującego, 100. Konfiguracja wydajności procesu backupu, 101. Zastępowanie nazwy pliku GUID-em, 102. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie

	komputera użytkownika, 103. Kompresja danych, 104. Transmisja po bezpiecznym protokole TLS, 105. Deklaracja klucza szyfrującego dane użytkownika, 106. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 107. Obliczanie sumy kontrolnej, 108. Kopie zapasowe musza być przechowywane w data center, na terenie Polski. 109. Licencje muszą być przypisywane do urządzenia z limitem pojemności przestrzeni w chmurze minimum 50 GB; 110. Wsparcie techniczne, świadczone w języku polskim; 111. Zarządzanie, monitoring, konfigurację oraz dystrybucję ustawień BIOS; 112. Oprogramowanie produkowane przez producenta komputera z nieograniczoną czasowo licencją umożliwiającą: 113. Upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji; 114. Mozliwość sprawdzenia każdego sterownika, aplikacji, BIOS'u bezpośrednio na stronie producenta przed instalacją oraz uzyskanie informacji o: a. poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodności z systemami operacyjnymi 115. Uzyskanie wylazu najnowszych aktualizacji z podziałem na krytyczne, rekomendowane i opcjonalne 116. Włączenie/wyłączenie funkcji automatycznego restartu; 117. Rozpoznanie modelu oferowanego komputera, numeru seryjnego, uzyskanie informacj kiedy dokonany został ostatnio upgrade; 118. Sprawdzenie historii upgrade'ów z informacją jakie sterowniki były instalowane; 119. Uzyskanie wykazu wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji; 120. Uzyskanie raportu uwzględniającego informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach

Zamawiający zastrzega sobie możliwość wezwania oferentów, którzy złożyli oferty niepodlegające odrzuceniu w niniejszym postępowaniu, do okazania zaoferowanego sprzętu i oprogramowania, w celu sprawdzenia ich zgodności z wymaganiami określonymi przez Zamawiającego w SIWZ.
Okazanie nastąpi w dniu wyznaczonym przez Zamawiającego, po terminie składania ofert. Zamawiający poinformuje o terminie przeprowadzenia okazania z co najmniej pięciodniowym wyprzedzeniem (dni kalendarzowe).
Niestawienie się oferenta w wyznaczonym czasie i miejscu na okazaniu (prezentacji) sprzętu i/lub oprogramowania, uznane będzie jako negatywny wynik okazania, tj. niepotwierdzenie przez

oferenta wymagań określonych przez Zamawiającego, co będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt. 5 Ustawy Pzp.