Załącznik nr 1 do zapytania ofertowego

S.042.2.2022

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa sprzętu komputerowego, sieciowego i oprogramowania na potrzeby Gminy Rutka-Tartak, w ramach projektu grantowego „Cyfrowa Gmina", w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina":

I. Rozbudowa zabezpieczeń logicznych (firewall, IPS)

II. Zintegrowane zarządzanie IT, oprogramowanie do infrastruktury sieciowej (backup i serwer NAS)

Część I , sprzętowa wchodząca w skład kompletnego, integralnego z częścią II systemu do kopii zapasowych / macierz główna.

Część II, software'owa wchodząca w skład kompletnego, integralnego z częścią I systemu do kopii zapasowych.

III. Zakup specjalistycznego oprogramowania – zarządzanie zasobami

IV. Doposażenie serwerowni.

Szafa serwerowa z wyposażeniem.

Serwer plików z licencjami

V. Stacje robocze z urządzeniami peryferyjnymi.

Stacje robocze:

Urządzenia peryferyjne:

VI. E-usługi dla mieszkańców

Oferowany sprzęt ma być fabrycznie nowy, nieużywany oraz nieeksponowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, a także musi

spełniać wymagania techniczno-funkcjonalne wyszczególnione w poniższym opisie przedmiotu zamówienia.

I. Rozbudowa zabezpieczeń logicznych (firewall, IPS)

OBSŁUGA SIECI

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

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

INTRUSION PREVENTION SYSTEM (IPS)

12. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
20. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

KSZTAŁTOWANIE PASMA (Traffic Shapping)

21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

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

OCHRONA ANTYSPAM

29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
30. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.
31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:

a. PPTP VPN,
b. IPSec VPN,
c. SSL VPN.

35. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
37. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
38. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
39. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

40. Urządzenie ma posiadać wbudowany filtr URL.
41. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
42. Administrator ma mieć możliwość dodawania własnych kategorii URL.
43. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
    a. blokowanie dostępu do adresu URL,
    b. zezwolenie na dostęp do adresu URL,
    c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
44. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
46. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
47. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
48. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE

49. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c. usługę katalogową Microsoft Active Directory.
50. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
51. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
    a. SSL,
    b. Radius,
    c. Kerberos.
52. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
53. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
54. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

55. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
56. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia.
57. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
58. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
59. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

60. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
61. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

62. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
63. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
64. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
65. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

66. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
67. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
68. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
69. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
70. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
71. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
72. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
73. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
74. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
75. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

a. manualnego eksportu do pliku w dowolnym momencie czasu,
b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

76. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
77. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

RAPORTOWANIE

78. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
79. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
80. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
81. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
82. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
83. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
84. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
85. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

86. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
87. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
88. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

89. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
90. Urządzenie ma posiadać usługę DNS Proxy.
91. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS

92. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
93. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

94. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
95. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
96. Liczba portów Ethernet 10/100/1000Mbps – min.8.
97. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
98. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
99. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2.4Gbps.
100. Przepustowość filtrowania Antywirusowego – minimum 495Mbps.
101. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 600Mbps.
102. Maksymalna liczba tuneli VPN IPSec – minimum 100.
103. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
104. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
105. Obsługa interfejsów 802.11q (VLAN) – minimum 128
106. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 18 000 nowych sesji/sekundę.

107. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
108. Urządzenie nie ma limitu na liczbę użytkowników.
109. Liczba reguł filtrowania – minimum 8 192.
110. Liczba tras statycznego routingu – minimum 512.
111. Liczba tras dynamicznego routingu – minimum 10 000.

II. Zintegrowane zarządzanie IT, oprogramowanie do infrastruktury sieciowej (backup i serwer NAS)

Część I , sprzętowa wchodząca w skład kompletnego, integralnego z częścią II systemu do kopii zapasowych / macierz główna.

1. Przeznaczenie: System do wykorzystana w ramach wykonywanej polityki backupu serwerów
2. Procesor: Procesor 64 bit Intel x86 o taktowaniu nie mniejszym niż 2.0 GHz
3. Liczba rdzeni nie mniej niż 4
4. Obudowa: 1U, Do montażu stelażowego w szafach Rack
5. Pamięć RAM Min. 4 GB DDR4
6. Pamięć Flash Nie mniej niż 4 GB
7. Ilość obsługiwanych dysków Minimum 4: 3.5" oraz 2.5" SATA oraz 2.5" SATA SSD
8. Możliwość podłączenia modułu rozszerzającego: minimum 2
9. Interfejsy sieciowe: minimum 2, prędkość 2,5 GbE
10. Wymagane porty USB 3.2 Gen2 (10 Gb/s)
11. Złącza PCIe: Min. 1x Gniazdo PCIe Gen 3
12. Wskaźniki LED Minimum Status, LAN, HDD
13. Przyciski: Min. Reset, Zasilanie
14. Zasilanie: Zasilacz redundantny 2 x 250W, 100-240 V
15. Agregacja łączy: Warunek niezbędny
16. Obsługiwane systemy plików: Dyski wewnętrzne: EXT4, Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
17. Szyfrowanie wolumenów: Min. AES 256
18. Szyfrowanie dysków zewnętrznych: Tak
19. Zarządzanie dyskami:

a. Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD,
b. Obsługa Hot Spare per grupa RAID oraz global hot spare
c. Rozszerzanie pojemności Online RAID
d. Migracja poziomów Online RAID
e. HDD S.M.A.R.T.
f. Skanowanie uszkodzonych bloków (pliku)
g. Przywracanie macierzy RAID
h. Obsługa map bitowych
i. Pula pamięci masowej
j. Obsługa migawek
k. Obsługa replikacji migawek

20. Wbudowana obsługa iSCSI:
    a. Multi-LUNs na Target
    b. Obsługa LUN Mapping & Masking
    c. Obsługa SPC-3 Persistent Reservation
    d. Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
21. Zarządzanie prawami dostępu:
    a. Ograniczenie dostępnej pojemności dysku dla użytkownika
    b. Importowanie listy użytkowników
    c. Zarządzanie kontami użytkowników
    d. Zarządzanie grupą użytkowników
    e. Zarządzanie współdzieleniem w sieci
    f. Tworzenie użytkowników za pomocą makr
    g. Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
22. Obsługa Windows AD
    a. Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web
    b. Funkcja serwera LDAP
23. Funkcje backup: Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,

24. Współpraca z zewnętrznymi dostawcami usług chmury: Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
25. Darmowe aplikacje na urządzenia mobilne:
    a. Monitoring
    b. Zarządzanie
    c. Współdzielenie plików
    d. Obsługa kamer
    e. Odtwarzacz muzyki

    Dostępne na systemy iOS oraz Android
26. Minimum obsługiwane serwery
    a. Serwer plików
    b. Serwer FTP
    c. Serwer WEB
    d. Serwer kopii zapasowych
    e. Serwer multimediów UPnP
    f. Serwer pobierania (Bittorrent / HTTP / FTP)
    g. Serwer Monitoringu
27. VPN: VPN client / VPN server. Obsługa PPTP, OpenVPN
28. Administracja systemu:
    a. Połączenia HTTP/HTTPS
    b. Powiadamianie przez e-mail (uwierzytelnianie SMTP)
    c. Powiadamianie przez SMS
    d. Ustawienia inteligentnego chłodzenia
    e. DDNS oraz zdalny dostęp w chmurze
    f. SNMP (v2 & v3)
    g. Obsługa UPS z zarządzaniem SNMP (USB)
    h. Obsługa sieciowej jednostki UPS
    i. Monitor zasobów
    j. Kosz sieciowy dla CIFS/SMB oraz AFP
    k. Monitor zasobów systemu w czasie rzeczywistym
    l. Rejestr zdarzeń

m. System plików dziennika
n. Całkowity rejestr systemowy (poziom pliku)
o. Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line
p. Możliwość aktualizacji oprogramowania
q. Ustawienia: Back up, przywracania ustawień, resetowania systemu

29. Wirtualizacja:
    a. Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.
    b. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5
    c. Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
30. Konteneryzacja: Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker
31. Zabezpieczenia:
    a. Filtracja IP
    b. Ochrona dostępu do sieci z automatycznym blokowaniem
    c. Połączenie HTTPS
    d. FTP z SSL/TLS (Explicit)
    e. Obsługa SFTP (tylko admin)
    f. Szyfrowanie AES 256-bit
    g. Szyfrowana zdalna replikacja (Rsync poprzez SSH)
    h. Import certyfikatu SSL
    i. Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
32. Możliwość instalacji dodatkowego oprogramowania: sklep z aplikacjami; możliwość instalacji z paczek
33. Komplet szyn przesuwnych
34. Dyski: 4 szt., dyski 4TB klasy NAS, znajdujące się na liście kompatybilności urządzenia, 3 lata gwarancji z opcją pozostawienia u klienta w przypadku awarii.
35. Gwarancja na NAS: Gwarancja 3 lata

Część II, software'owa wchodząca w skład kompletnego, integralnego z częścią I systemu do kopii zapasowych.

Ogólne:

1. Oprogramowanie może być dostarczane w dwóch scenariuszach:
    a. Cloud(Software as Service),
    b. On-premise.
2. Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.
3. Interfejs systemu dostępny jest w języku:
    a. polskim,
    b. angielskim,
4. Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych,
5. Oprogramowanie może być uruchomione w kontenerze docker,
6. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
    a. Debian: 9+
    b. Ubuntu: 16.04+
    c. Fedora: 29+
    d. centOS: 7+
    e. RHEL: 6+
    f. openSUSE: 15+
    g. SUSE Enterprise Linux (SLES): 12 SP2+
    h. Windows Client: 7, 8.1, 10 (1607+)
    i. Windows Server: 2012 R2+
    j. Windows Server: 2008 R2, 2012
7. System automatycznie wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,
8. Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju),

Wsparcie techniczne:

9. Pomoc techniczna w językach:
    a. polskim,
    b. angielskim.
10. Materiały samopomocowe:
    a. Baza wiedzy:
        i. polski,
        ii. angielski
11. Wsparcie techniczne zawiera wsparcie inżyniera producenta w zakresie rozwiązywania problemów konfiguracyjnych oraz technicznych w Systemie w miejscu jego użytkowania.
12. Wsparcie techniczne zawiera wsparcie świadczone telefoniczne oraz poprzez system zgłoszeń przez producenta, a także dostęp do nowych wersji oprogramowania.

Zarządzanie:

13. Zarządzanie całością działania systemu(backup, przywracanie)z poziomu jednej konsoli webowej,
14. Zarządzanie całym systemem poprzez dashboardy,
15. Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,
16. System posiada wbudowane predefiniowane zadania backupowe,
17. System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.
18. Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,
19. Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,
20. Monitorowanie postępu działania zadania,
21. Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:
    a. Zadanie zostało zakończone pomyślnie,
    b. Zadanie zostało zakończone z ostrzeżeniami,
    c. Zadanie zostało zakończone z błędem,

   d. Zadanie zostało anulowane,
   e. Zadanie nie zostało uruchomione.
22. System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
23. Możliwość zdefiniowania okna backupowego dla każdego z zadań,
24. Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,
25. System pozwala na skonfigurowanie podwójnej autentyfikacji administratora(2FA),
26. System pozwala na klonowanie planów kopii zapasowych,
27. System umożliwia reset hasła administratora w przypadku jego utraty,
28. Oprogramowanie umożliwia definiowanie retencji według schematów:
   a. GFS(Grandfather-Father-Son),
   b. FIFO(First-In, First-Out).
29. Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,
30. Konta użytkowników mogą być tworzone poprzez import pliku CSV,
31. Każdy użytkownik posiada możliwość odtwarzania swoich danych,
32. Oprogramowanie umożliwia tworzenie grup urządzeń,
33. Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
34. Oprogramowanie pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in. :
   a. System Administrator,
   b. Backup operator,
   c. Restore operator,
   d. Viewer.

Składowanie danych:

35. Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie,

36. Oprogramowanie umożliwia składowanie danych:
    a. Lokalnie:
        i. Zasób SMB,
        ii. Zasób NFS,
        iii. Katalog zabezpieczonego urządzenia.
    b. W chmurze:
        i. Amazon Web Service,
        ii. Magazyn zgodny z S3,
        iii. Producenta oprogramowania,
37. System umożliwia replikację repozytoriów do innych lokalizacji,
38. System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,
39. System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.

Odtwarzanie:

40. Odtwarzanie granularne:
    a. Pojedynczych plików z kopii obrazu dysku,
    b. Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365,
41. Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
    a. Windows: 7, 8.1, 10(1607+),
    b. Windows Server: 2012 R2+,
    c. Windows Server: 2008 R2, 2012.
42. Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
43. Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a,
44. Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.

45. Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),
46. Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),
47. Odtwarzanie zasobów plikowych z prawami dostępu,
48. Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows),
49. Odtwarzanie danych według harmonogramu,
50. Przywracanie danych z określonego urządzenia/użytkownika,
51. Przywracanie kopii z wybranego magazynu.
52. Przywracanie danych Microsoft 365:
    a. do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku:
        i. pst,
        ii. mbox.
    b. do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),
53. System posiada możliwość nieodwracalnego kasowania danych,
54. Przywracanie repozytoriów GIT:
    a. Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket/GitLAB),
    b. przywracanie między kontami.

Backup:

55. Środowisk wirtualnych:
    a. VMware: 6.0+.
56. Usługi Microsoft 365:
    a. Skrzynki pocztowe,
    b. Kontakty,
    c. Kalendarze,
    d. OneDrive,
57. Repozytoriów GIT:
    a. GitHub,
    b. GitLab,

c. Bitbucket.Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:
    i. Systemów operacyjnych:
        1. Alpine 3.10+,
        2. Debian: 9+,
        3. Ubuntu: 16.04+,
        4. Fedora: 29+,
        5. centOS: 7+,
        6. RHEL: 6+,
        7. openSUSE: 15+,
        8. SUSE Enterprise Linux(SLES): 12 SP2+,
        9. macOS: 10.13+,
        10. Windows: 7, 8.1, 10(1607+),
        11. Windows Server: 2012 R2+,
        12. Windows Server: 2008 R2, 2012.

58. Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:
    a. Baz danych:
        i. Microsoft SQL,
        ii. MySQL,
        iii. PostgreSQL,
        iv. Firebird,
        v. Oracle.
59. Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:
    a. 128 bit,
    b. 192 bit,
    c. 256 bit.
60. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:
    a. ZStandard,
    b. LZ4.

61. Oprogramowanie umożliwia zarządzanie poziomem kompresji,
62. Wykonywanie kopii zapasowej otwartych plików(VSS),
63. System umożliwia uruchamianie skryptów przed i po backupie,
64. System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,
65. System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,
66. Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,
67. Backup plikowy,
68. Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,
69. Oprogramowanie umożliwia konsolidację wersji kopii zapasowych,
70. Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,
71. Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.

Vmware:

72. System wspiera mechanizm CBT(change block tracking) dla VMware,
73. Application-aware backup,
74. Oprogramowanie nie wymaga żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej,

Licencje:

75. 15 licencji typu desktop, 1 licencje typu serwer (Windows, Linux) Dożywotnie

Wsparcie techniczne dla części I-ej:

76. Wsparcie techniczne minimum 12 miesięcy
    a. pomoc telefoniczna lub e-mailowa przy uruchomieniu i wdrożeniu produktu,
    b. wsparcie techniczne w przypadku problemów ze współpracą z innymi elementami sieci,
    c. powiadomienie o dostępnych aktualizacjach dla zakupionego produktów,
    d. pełna asysta telefoniczna / e-mailowa przy aktualizacji oprogramowania,

e. gwarancja „door-door" w całości pokrywana przez serwis,

f. priorytetowy tryb rozpatrywania gwarancji i prowadzenia naprawy.)

Wdrożenie:

77. Wdrożenie realizowane jest bezpośrednio przez producenta oprogramowania,
78. Wdrożenie realizowane jest w formie zdalnej,
79. Komunikacja musi odbywać się w języku polskim,
80. Wdrożenie obejmuje pełną konfigurację wszystkich aplikacji niezbędnych do uruchomienia zadań backupu oraz uruchomienie tych zadań,
81. Czas wdrożenia nie jest ograniczony
82. Wdrożenie zakończone jest szkoleniem z obsługi oprogramowania zakończone certyfikatem dla administratora systemu wystawionym bezpośrednio przez producenta oprogramowania

III. Zakup specjalistycznego oprogramowania – zarządzanie zasobami

Wymagania ogólne dla systemu zarządzania

1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
2. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
3. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
4. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
5. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
6. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.

7. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
8. Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
9. Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
10. Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
11. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
12. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .
13. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie przypisywania wybranych jednostek organizacyjnych, Jednostek lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty.
14. Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).
15. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
16. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
17. Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
18. Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).

19. Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
20. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
21. Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
22. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
23. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
24. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
25. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
26. Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień, predefiniowane atrybuty komputera.
27. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.
28. Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
29. Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.

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

Inwentaryzacja konfiguracji komputerów

31. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
32. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
33. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
34. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
35. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
36. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
37. Oprogramowanie musi umożliwiać analizę sprzętową:
    a. płyty głównej w zakresie model, producent, nr. seryjny,
    b. CPU w zakresie nazwy, modelu, producenta, częstotliwości,
    c. HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
    d. RAM w zakresie wielkości pamięci,
    e. karty sieciowej w zakresie model, adres IP, adres MAC,
    f. karty graficznej w zakresie model.
38. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
39. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.

40. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
41. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
42. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
43. Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
44. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

Inwentaryzacja oprogramowania

45. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
46. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
47. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
48. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
49. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
50. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
51. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
52. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
53. Oprogramowanie musi umożliwiać okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów.

54. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
55. Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

Zarządzanie licencjami, audyt oprogramowania

56. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania\
57. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe).
58. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
59. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
60. Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

Zdalny pulpit, zdalne zarządzanie komputerem

61. Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
62. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
63. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).

64. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
65. Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
66. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
67. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
68. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
69. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
70. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
71. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
72. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
73. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
74. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
75. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
76. Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.
77. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Automatyzacja

78. Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów

lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.

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

88. Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.
89. Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
90. Oprogramowanie musi umożliwiać optymalizację dystrybucji zadań oraz plików na komputery, pobierając brakujące fragmenty plików od agentów z tej samej podsieci (mechanizm peer-to-peer).
91. Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
    a. Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
    b. Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
    c. Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi
    d. Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
    e. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.

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

Zarządzanie urządzeniami USB Storage

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

Monitoring użytkowników

97. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
98. Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
99. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
100. Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
101. Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
102. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
103. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
104. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
105. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.

106. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
107. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
108. Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
109. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
110. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.
111. Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.
112. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

Monitoring sieci LAN

113. Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony
114. Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.

115. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
116. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
117. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
118. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
119. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
120. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

Zarządzanie urządzeniami komputerowymi z systemem MacOS:

121. Oprogramowanie musi umożliwiać skanowanie komputerów z systemem MacOS w zakresie konfiguracji sprzętowej oraz zainstalowanego oprogramowania
122. Oprogramowanie musi umożliwiać, z listy stanowisk zarejestrowanych w konsoli systemu stanowisk, przejęcie pulpitu wybranego komputera

System wewnętrznego komunikatora dla użytkowników

123. Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.
124. Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostrgeSQL
125. Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.
126. Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami

127. Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.
128. Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.
129. Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).
130. Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.
131. Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).
132. Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.
133. Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.
134. Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).
135. Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami
136. Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.

Wymagania formalne:

137. Dostarczone licencje na oprogramowanie muszą być bezterminowe.
138. Dostarczone licencje na oprogramowanie muszą być dostarczone z 12 miesięcznym supportem producenta, liczonym od daty zakończenia wdrożenia.
139. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
140. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 15 stanowisk komputerowych z systemem klasy Microsoft Windows. Licencje nie mogą mieć ograniczeń

ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencji dostępową do konsoli zarządzającej.

IV. Doposażenie serwerowni.

Szafa serwerowa z wyposażeniem.

1. Wymiary zewnętrzne szafy: 800x1000x2050 [mm] – (szer. x gł. X wys.)
2. Cechy szafy:
    a. materiał: stal walcowana na zimno, malowana na kolor czarny (RAL 9004),
    b. drzwi frontowe (przednie) - przeszklone (szkło hartowane) z zamkiem i klamką
    c. możliwość montażu drzwi jako lewych bądź prawych,
    d. drzwi tylne - pełne stalowe z zamkiem,
    e. drzwi boczne (panele) - pełne stalowe demontowane na zatrzaskach,
    f. w zestawie komplet kluczyków,
    g. złącze uziemiające,
    h. dedykowany cokół 800x1000 mm,
    i. 1 wysuwana półka o głębokości 1000mm
    j. możliwość montażu urządzeń o sumarycznej wysokości 42u,
    k. maksymalne obciążenie szkieletu do 800kg (nośność statyczna),
    l. kompatybilne ze standardami: metrycznym, ETSI oraz międzynarodowym 19”
    m. szafę przemieszcza się na kółkach jezdnych, stabilizuje się wykręcając 4 nogi,
    n. gwarancja 2 lata
3. Dodatkowe wyposażenie: jednostka wentylacyjna złożona z 4 wentylatorów, z termostatem z wyświetlaczem LED, przeznaczona do montażu w szafie Rack 19", wysokość montażowa 1U - patchpanel RACK 19" 5e 24porty UTP.

Serwer plików z licencjami

Obudowa

1. 1U
2. Obudowa serwerowa do montażu w szafie RACK 19" wraz z wysuwanymi szynami dedykowanymi do tego urządzenia przez producenta serwera.
3. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

4. Obudowa powinna posiadać możliwość instalacji interfejsu NFC do połączenia z aplikacją zarządzającą serwerem na telefonie.
5. Aplikacja zarządzająca powinna być dostępna na Android i iOS
6. obudowa powinna posiadać dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.
7. Musi istnieć możliwość rozbudowy o panel pokazujący stan działania serwera w tym jego adres IP
8. W obudowie powinien być zaistalowany zestaw redundantnych zasilaczy o mocy co najmniej 800W każdy wymienialnych podczas pracy oraz zestaw redundantnych wentylatorów.
9. Wentylatory powinny mieć możliwość wymiany podczas pracy systemu

Płyta główna

10. Płyta główna obsługująca co najmniej dwa procesory i co najmniej 16 slotów na pamięć taktowaną przynajmniej z częstotliwością 3200MT/s przy użyciu odpowiednich procesorów.
11. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
12. Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0

Procesor

13. Procesor typu skalowalnego posiadający co najmniej 10 rdzeni działający co najmniej z częstotliwością 2.3GHz i dający w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/, wynik nie mniejszy niż 20950

Pamięć RAM

14. 64 GB pamięci RAM w modułach 32GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 3200MT/s

Dyski

15. Miejsce na co najmniej 8 dysków w rozmiarze 2.5", wymienialne bez wyłączania systemu.
16. Serwer ma mieć przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski.

17. Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0,1,5,10,50,6 posiadający co najmniej 2GB pamięci cache zabezpieczonej przed awarią prądu.
18. W serwerze powinny być zainstalowane co najmniej trzy dyski co najmniej 480GB SSD

Sieć

19. Na płycie głównej powinna być zainstalowana dwuportowa karta sieciowa 1GB BT
20. Karta nie może zajmować slotu PCIe

Karta zarządzająca

21. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    a. zdalny dostęp do graficznego interfejsu Web karty zarządzającej
    b. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika
    c. możliwość podmontowania zdalnych wirtualnych napędów
    d. wirtualną konsolę z dostępem do myszy, klawiatury
    e. wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH
    f. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.
    g. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
    h. integracja z Active Directory
    i. możliwość obsługi przez ośmiu administratorów jednocześnie
    j. Wsparcie dla automatycznej rejestracji DNS - wsparcie dla LLDP
    k. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
    l. możliwość podłączenia lokalnego poprzez złącze RS-232.
    m. możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.
    n. Monitorowanie zużycia dysków SSD
    o. możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,
    p. Automatyczne zgłaszanie alertów do centrum serwisowego producenta
    q. Automatyczne update firmware dla wszystkich komponentów serwera
    r. Możliwość przywrócenia poprzednich wersji firmware

s. Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
t. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych
u. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.

Certyfikaty

22. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.
23. Serwer musi posiadać deklarację CE.
24. System operacyjny – Windows Server 2022,Essentials Edition,ROK,10CORE (for Distributor sale only)

Warunki gwarancji

3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia - zgłoszenia przyjmowane 7 dni w tygodniu w trybie 24/7.
Gwarancja musi obejmować całość rozwiązania nie powinno być tak aby jakaś część tego rozwiązania nie podlegała gwarancji.
Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.
Producent musi dawać możliwość rozszerzenia gwarancji do 7 lat
W przypadku naprawy dysku - uszkodzony dysk zostaje u klienta.
Podczas trwania gwarancji producent powinien zapewnić narzędzia i procesy do proaktywnej oceny stanu technicznego, oraz automatycznego zgłaszania usterek bez ingerencji człowieka.
Powinna być możliwość skorzystania z pomocy wsparcia producenta za pomocą komunikatora np. Messenger, MSteams, WhatsApp.
Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.
Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

V. Stacje robocze z urządzeniami peryferyjnymi.

Stacje robocze:

1. Procesor: Intel® Core™ i5-12400 (18MB Cache; 2,50 - 4,40GHz) lub równoważny
2. Pamięć RAM: 16GB DIMM DDR4 3200MHz
3. Dysk twardy: SSD 256GB M.2 NVMe
4. Napęd optyczny: Nagrywarka DVD+/-RW DualLayer
5. Karta grafiki: Intel® UHD Graphics 730 lub równoważna
6. System operacyjny: Windows 11 Professional
7. Inne: Display Port, HDMI, USB 3.0,

Urządzenia peryferyjne:

1. Klawiatura i mysz – bezprzewodowe
2. Monitor:
    a. LCD Full HD
    b. Typ panelu LCD: Technologia IPS
    c. Typ wyświetlacza: System W-LED
    d. Rozmiar panelu: 68,6 cm / 27 cali
    e. Powłoka ekranu: Przeciwodblaskowa, 3H, Haze 25%
    f. Część widoczna ekranu: 597,89 (w poziomie) x 336,31 (w pionie)
    g. Format obrazu: 16:9
    h. Maks. Rozdzielczość: 1920 x 1080 przy 75 Hz
    i. Gęstość pikseli: 82 PPI
    j. Czas reakcji (standardowy): 4 ms (szarości)*
    k. Jasność: 250 cd/m²
    l. SmartContrast: 10 000 000:1
    m. Współczynnik kontrastu (typowy): 1000:1
    n. Rozmiar plamki: 0,311 x 0,311 mm
    o. Kąt widzenia: 178º (poz.) / 178º (pion.) przy C/R > 10
    p. Bez efektu migotania: Tak
    q. Kolory wyświetlacza: 16,7 M

r. Częstotliwość odświeżania: 30–83 kHz (poz.) / 56–76 Hz (pion.)
s. Tryb LowBlue: Tak
t. sRGB: Tak
u. Wejście sygnału: HDMI (cyfrowe HDCP)
v. Przewody: Przewód HDMI, przewód zasilający

Zamawiający wymaga, aby oferowany sprzęt komputerowy był fabrycznie nowy, wcześniej nieużywany, wolny od wad i nieobciążony prawami osób trzecich.

VI. E-usługi dla mieszkańców

Aplikacja umożliwiająca wysyłanie spersonalizowanych SMS-ów do podatników, posiadająca co najmniej następujące funkcje:

1. Wybór adresatów powiadomień wg danych z bazy osobowej
2. Predefiniowane szablony wiadomości
3. Automatyczne personalizowanie wiadomości w oparciu o informacje wymiarowe i księgowe
4. Eksportowanie danych gotowych do wysyłki SMS do pliku Szablon komunikatu
5. Dowolne redagowanie treści powiadomienia
6. Kontrola wysyłki – możliwe wcześniejsze przeglądanie i weryfikacja przygotowanych powiadomień
7. Integracja z aplikacjami dziedzinowymi INFO-SYSTEM

Wszelkie wskazania, odniesienia do znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, znajdujące się w niniejszym opisie przedmiotu zamówienia należy traktować jako przykład. Zamawiający uzna za prawidłowe jeśli proponowane przez oferenta rozwiązania w równoważnym stopniu spełniają wymagania określone w zapytaniu ofertowym.

Piotr Sinkiewicz
Elektronicznie podpisany przez Piotr Sinkiewicz
Data: 2022.12.09 12:09:50 +01'00'