**Załącznik nr 7 – Dokumentacja techniczna**

## I. Przełącznik sieciowy - Typ I – 2 szt.

Urządzenia sieciowe i osprzęt sieciowy pozwalający na przyłączenie do szerokopasmowego Internetu.
Przełącznik musi posiadać co najmniej następujące funkcjonalności:

1. Porty:
   48x 10/100/1000Base-T oraz 4 porty 10GE SFP+; Porty SFP+ 10GE obsługujące moduły 1GE SFP;
2. Stackowanie:
   Możliwość połączenia 4 przełączników w stos za pomocą portów SFP+ bez okablowania
3. Port konsolowy: RJ45 (RS-232)
4. Port zarządzania: RJ45 (10/100Base-T RJ45)
5. Port USB: 1 port w standardzie 2.0
6. Szybkość przełączania: 175 Gb/s
7. Przepustowość: 130 Mp/s
8. Bufor pakietów: 1,5MB
9. Ramki Jumbo: 10k
10. Tablica adresów MAC: 16k
11. Adresy MAC – Multicast: 1k
12. Tablica ACL: 256
13. Tablica VLAN: 4094
14. Tablica routingu: 512 dla IPv4, w tym IPv6.
    Dopuszcza się rozwiązania współdzielące tablicę routingu dla IPv4 oraz IPv6 w maksymalnej proporcji 4:1.
15. Tablica ARP: 512
16. Taktowanie procesora: 800MHz
17. Pamięć Flash: 128MB
18. Pamięć RAM: 256MB
19. Obsługa PoE: IEEE 802.3 af/at
20. Budżet mocy PoE: 740W
21. Redundantne zasilanie;
22. Pobór mocy podczas pracy: maksymalnie 900W
23. Zabezpieczenie przeciwprzepięciowe: 4kV
24. Obsługa VLAN:
    Voice VLAN, VLAN oparty na portach, protokołach i MAC adresie, prywatny VLAN, GVRP, IEEE 802.1Q, standardowy i elastyczny QinQ;
25. DHCP:
    IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 serwer DHCP;
26. Protokoły drzewa rozpinającego:
    IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, BPDU guard, BPDU forwarding,
27. Protekcja ringowa:
    ITU-T G.8032 – czas przywracania time < 50ms, Loopback Detection, Fast Link
28. Protokoły routingu:
    statyczny Routing, RIPv1/v2, RIPng, OSPFv2/v3, BGP4, BGP4+, OSPF multiple process, LPM Routing, Policy-based Routing (PBR) IPv4/IPv6, VRRP, IPv6 VRRPv3, URPF IPv4/IPv6, ECMP, BFD, Static Multicast Route, Multicast Receive Control, Illegal Multicast Source Detect

29. Agregacja linków:
    IEEE 802.3ad (LACP), 64 grup na urządzenie / 8 portów na grupę, load balance
30. Bezpieczeństwo:
    Storm Control oparty na pakietach, port Security, MAC Limit oparty o VLAN I porty, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, uwierzytelnianie, autoryzacja, Radius IPv4/IPv6, TACACS+, MAB, autentykacja oparta na portach I MAC adresie, gościnna sieć VLAN i auto VLAN,
31. Multicast:
32. IGMP v1/v2/v3 snooping i zapytania L2, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, autentykacja IGMP;
33. QoS: 8 kolejek na port, kontrola pasma i ruchu: HOL, IEEE802.3x, przekirowanie ruchu, klasyfikacja oparta na ACL, COS, TOS, DiffServ, DSCP, numeracja portów; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, klient DNS, DNS Relay
34. Lista kontroli dostępu: IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, ACL definiowany przez uzytkownika, Time Range ACL, numeracja portów TCP/UDP ACL, VLAN ACL, statystyki i przekierowania oparte o ACL, Vlan Tag/Untag, reguły konfigurowane dla portu i VLAN
35. Diagnostyka: sFlow, analiza ruchu, VCT, Ping, Trace Route,
36. Zarządzanie: TFTP/FTP, CLI, Telnet, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, publiczny i prywatny interfejs MIB, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Port Mirror, IEEE 802.3ah OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF;
37. Oprogramowanie oraz wsparcie techniczne:
    OIprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, przez Internet, wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług
38. Gwarancja: 36 miesięcy

## II. Przełącznik sieciowy - Typ II – 3 szt.

Urządzenia sieciowe i osprzęt sieciowy pozwalający na przyłączenie do szerokopasmowego Internetu.
Przełącznik musi posiadać co najmniej następujące funkcjonalności:

1. Ilość portów 24 porty PoE+ 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
2. Chłodzenie od przodu do tyłu obudowy
3. Budżet mocy PoE - 480W
4. Tablica MAC - 16K
5. Tablica ARP/NDP - 888
6. Bufor - 16Mb
7. MTBF – 1 100 000 godzin
8. Wydajność - 95 Mp/s
9. Przepustowość - 128 Gb/s
10. Porty – 1 x USB, 1 x miniUSB, 1 x port zarządzania Out-of-band;
11. Web GUI
12. HTTPs
13. CLI
14. Telnet
15. SSH
16. SNMP
17. MIB RSPAN
18. Radius

19. TACACS+
20. DiffServ
21. Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
22. IPv4/IPv6 Multicast filtering
23. IGMPv3 MLDv2 Snooping
24. ASM & SSM
25. IGMPv1,v2 Querier
26. Auto-VoIP
27. Auto-iSCSI
28. Policy-based routing (PBR)
29. LLDP-MED
30. Spanning Tree
31. Green Ethernet
32. STP
33. MTP
34. RSTP
35. PV(R)STP
36. BPDU/STRG Root Guard
37. EEE (802.3az)
38. GVRP/GMRP
39. Q in Q,
40. Private VLAN
41. DOT1X
42. MAB
43. Captive Portal
44. DHCP Snooping
45. Dynamic ARP
46. Inspection
47. IP Source Guard
48. Procesor - 800 Mhz
49. RAM - 1GB
50. Flash - 256MB;
51. Ilość obsługiwanych VLAN – 4 tys.
52. DHCP Server – 2 tys. rezerwacji
53. Ilość przełączników w stosie - 8
54. Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
55. Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
56. Non-stop forwarding (NSF)
57. Distributed Link Aggregation;
58. Ilość interfejsów IP - 128
59. Double VLAN Tagging (QoQ)
60. Multicast Routing;
61. IPv6
62. RIPv2
63. OSPFv2
64. RFC 2328
65. RFC 1583
66. OSPFv2 I 3
67. UDLD
68. LLPF
69. DHCPv6 Snooping
70. wysyłanie alertów na email

71. MMRP
72. Ilość list ACL - 100
73. Ilość reguł na listę - 1023 na wejściu
74. Zasilacz z certyfikatem 80+
75. Urządzenie musi być objęte wieczystą gwarancją producenta, do 5 lat po ogłoszeniu końca jego produkcji;
76. Serwis realizowany w systemie door-to-door przez serwis producenta;
77. Urządzenie musi być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii;

## III. Serwer – 1 szt.

| Nazwa komponentu | Wymagane minimalne parametry techniczne |
|---|---|
| Obudowa | Typu Rack, wysokość maksymalnie2U;<br>Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack. Możliwość montażu ramienia porządkującego przewody. |
| Płyta główna | Dwuprocesorowa, wyprodukowana przez producenta serwera; Możliwość instalacji procesorów 14-rdzeniowych;<br>6 złącz PCI Express, w tym 3 złącza o prędkości PCI Express x16 generacji 3;<br>Zainstalowany moduł TPM 2.0 kompatybilny z oferowanym systemem operacyjnym; |
| Procesory | Zainstalowany procesor, osiągający w teście PassMark Average CPU Mark wynik 13 100 pkt. – **załączyć do oferty wydruk ze strony www.cpunechmark.net** |
| Pamięć RAM | Zainstalowane 128 GB pamięci RAM DDR4 typu Registered, 2933Mhz w kościach o pojemności 32 GB;<br>Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC;<br>12 gniazd pamięci RAM na płycie głównej, obsługa minimum 768 GB pamięci RAM; |
| Kontrolery dyskowe, I/O | Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,10,50,60; |
| Dyski twarde | Zainstalowanych 8 dysków SAS o pojemności 2,4 TB każdy, dyski Hotplug;<br>8 wnęk dla dysków twardych Hotplug 2,5”; |
| Inne napędy zintegrowane | Możliwość montażu napędu optycznego typu DVD-RW; |
| Kontrolery LAN | Wbudowana w płytę główną karta 2 x 1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express; |
| Porty | Zintegrowana karta graficzna ze złączem VGA;<br>7 x USB 3.0, w tym minimum 2 na panelu przednim, minimum 1 wewnętrzne; |
| Zasilanie, chłodzenie | Dwa redundantne zasilacze hotplug o sprawności. klasa Platinum, o mocy maksymalnej 800W każdy;<br>Redundantne wentylatory;<br>Dwa kable zasilające C13-C14 o długości 4m każdy; |
| Zarządzanie | Wbudowane diody informacyjne informujące o stanie serwera;<br>Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:<br>1. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; |

| | |
|---|---|
| | 2. Dedykowana karta LAN 1 Gb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;<br>3. Dostęp poprzez przeglądarkę Web;<br>4. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;<br>5. Zarządzanie alarmami (zdarzenia poprzez SNMP);<br>6. Możliwość przejęcia konsoli tekstowej;<br>7. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);<br>8. Możliwość pobrania darmowego oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera umożliwiającego konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (minimum temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.);<br>9. Zainstalowana, dedykowana dla potrzeb karty zarządzającej pamięć flash o pojemności 16 GB;<br>10. Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci o pojemności 8 GB;<br>11. Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania;<br>12. Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;<br>13. Możliwość konfiguracji i wykonania aktualizacji BIOS, firmware, sterowników serwera bezpośrednio z GUI karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej, a w szczególności bez pendrive, dysków twardych<br>14. Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń);<br>15. Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej. Dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą;<br>16. Karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce. W(wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta |

| | |
|---|---|
| | serwera, nie dopuszcza się komunikacji SNMP czy email. Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty. |
| Gwarancja | 5 lat gwarancji producenta serwera w trybie onsite z czasem reakcji w miejscu instalacji sprzętu najpóźniej w następnym dniu roboczym od zgłoszenia usterki;<br>Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;<br>Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera.<br>Jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera taka licencja musi być uwzględniona w konfiguracji;<br>Zgłoszenia serwisowe w języku polskim na dedykowany nr infolinii serwisowej producenta serwera;<br>Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera |
| Dokumentacja, inne | Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – **załączyć do oferty oświadczenie producenta serwera potwierdzające spełnienie tego wymagania;**<br>Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Unii Europejskiej – **załączyć do oferty oświadczenie producenta serwera potwierdzające spełnienie tego wymagania;**;<br>Ogólnopolska, telefoniczna, polskojęzyczna infolinia/linia techniczna producenta serwera. W czasie obowiązywania gwarancji na sprzęt umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. |
| System operacyjny | Licencja musi uprawniać do zainstalowania w środowisku fizycznym lub dwóch instancji wirtualnych;<br>Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.<br>1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.<br>2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.<br>3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.<br>4) 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.<br>5) Dodawanie i wymiana pamięci RAM bez przerywania pracy.<br>6) Dodawanie i wymiana procesorów bez przerywania pracy. |

| | |
|---|---|
| | 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.<br>8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.<br>9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:<br>a) pozwalają na zmianę rozmiaru w czasie pracy systemu,<br>b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,<br>c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,<br>d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).<br>10) Wbudowany mechanizm klasyfikowania i indeksowania plików w oparciu o ich zawartość.<br>11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.<br>12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET<br>13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.<br>14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.<br>15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.<br>16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,<br>17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu;<br>18) Mechanizmy logowania w oparciu o:<br>a) Login i hasło,<br>b) Karty z certyfikatami (smartcard),<br>c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),<br>19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..<br>20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).<br>21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |

| | |
|---|---|
| | 22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.<br>23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach;<br>24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.<br>25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:<br>a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,<br>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), z możliwością wykorzystania następujących funkcji:<br>i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,<br>ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,<br>iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.<br>iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych;<br>c) Zdalna dystrybucja oprogramowania na stacje robocze.<br>d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej<br>e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:<br>i. Dystrybucję certyfikatów poprzez http<br>ii. Konsolidację CA dla wielu lasów domeny,<br>iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,<br>iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.<br>f) Szyfrowanie plików i folderów.<br>g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).<br>h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.<br>i) Serwis udostępniania stron WWW.<br>j) Wsparcie dla protokołu IP w wersji 6 (IPv6),<br>k) Wsparcie dla algorytmów Suite B (RFC 4869),<br>l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach;<br>m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez |

| | |
|---|---|
| | zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.<br>n) Mechanizmy wirtualizacji mają zapewnić wsparcie dla:<br>i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,<br>ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.<br>iii. Obsługi 4-KB sektorów dysków<br>iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra<br>v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.<br>vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)<br>26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.<br>27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek;<br>28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.<br>29) Mechanizmy zdalnej administracji oraz mechanizmy administracji przez skrypty.<br>30) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |

## IV. Infokiosk zewnętrzny – 1 szt.

Infokiosk - urządzenie informujące o zakresie działalności urzędu, rozmieszczeniu pomieszczeń w budynku, zapewnieniu dostępności dla osób o szczególnych potrzebach.

1. Przekątna wyświetlacza: 55”
2. Jasność: 3000 cd/m2
3. Rozdzielczość: 1920x1080
4. Kontrast: 1000:1
5. Proporcje ekranu: 16:9
6. Kąt widzenia : 178 x 178
7. Zdolność do pracy: 24/7
8. Czas reakcji matrycy: 6ms
9. Ekran dotykowy pojemnościowy wykrywający 10 pkt. dotyku
10. Głośniki wbudowane w obudowę
11. Temperaturowy zakres pracy: - 30°C do +50°C
12. Wbudowany komputer o następujących parametrach:
    a) **Procesor osiągający w teście PassMark Average CPU Mark wynik 11 000 pkt. – załaczyć do oferty wydruk ze strony www.cpubenchmark.net lub www.passmark.com;**
    b) RAM: 8GB DDR4
    c) Dysk twardy: 120GB SSD

d) System operacyjny klasy PC spełniający następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
- 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
- Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego
- Interfejs użytkownika dostępny w języku polskim i angielskim
- Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
- Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
- Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego;
- System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
- Graficzne środowisko instalacji i konfiguracji w języku polskim
- Wbudowany system pomocy w języku polskim.
- Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
- Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego.
- Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
- Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
- Zabezpieczony hasłem hierarchiczny dostęp do systemu;
- Konta i profile użytkowników zarządzane zdalnie;
- Praca systemu w trybie ochrony kont użytkowników.
- Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze;
- Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
- 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
- Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
- Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
- Oprogramowanie dla tworzenia kopii zapasowych (Backup);
- Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
- Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.

- Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
- Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
- Wbudowany mechanizm wirtualizacji typu hypervisor;
- Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego.
- Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego.
- Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych;
- Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
- Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny;
- Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików;
- Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików.
- Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi.
- Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne;
- Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
- Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych;
- Możliwość tworzenia wirtualnych kart inteligentnych.
- Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
- Wsparcie dla IPSEC oparte na politykach;
- Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
- 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;
- Umozliwiajacy pracę w domenie;

13. Konstrukcja wolnostojąca, FULL OUTDOOR (IP65) z aluminium/stal, lakierowana na dowolny kolor z palety RAL.
    a) Konstrukcja słupa: stal ocynkowana, pokryta aluminium malowana proszkowo.
    b) Skrzydło drzwiowe: rama aluminiowa, szkło hartowane o grubości: 8 mm.
    c) System wentylacji filtrami,
    d) Ogrzewacz z termostatem,
    e) Bezpieczniki, gniazdka, przewody uszczelki;
    f) Odtwarzacz z dożywotnią licencją na oprogramowania
    g) Oprogramowanie umożliwiające zdalne sterowanie przez Internet
    h) Odtwarzanie plików graficznych i plików audio/wideo;
    i) Prezentacja i edycja własnych treści w formacie tekstowym
    j) Kreator treści reklamowych
    k) Możliwość odtwarzania dźwiękowego treści przez osoby słabowidzące po dotknięciu dłonią miejsca na ekranie umożliwiającego odtworzenie dźwięków
    l) Możliwość montażu 3 fizycznych przycisków funkcyjnych do obsługi kiosku przez osoby na wózku inwalidzkim
14. Gwarancja – 2 lata w miejscu instalacji urzadzenia

## V. Laptop z oprogramowaniem – 15 szt.

| Nazwa komponentu | Wymagane minimalne parametry techniczne |
|---|---|
| Zastosowanie | Sprzęt ma być przeznaczony dla radnych Rady Miejskiej w Gubinie. Urządzenia będą wykorzystywane do prowadzenia zdalnych sesji Rady Miejskiej,posiedzeń komisji, szkoleń prowadzonych w trybie online.<br>Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej |
| Ekran | 15.6 FHD IPS lub VA (1920 x 1080), powłoką przeciwodblaskową, jasność 220 nits |
| Wydajność | Komputer w oferowanej konfiguracji musi osiągać w teście wydajności PC Mark 10 wynik 4000 pkt. **Wydruk z oprogramowania testującego załączyć do oferty.**<br>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.).<br>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 | 8GB z możliwością rozbudowy do 32GB RAM. |
| Pamięć masowa | 256GB NVMe SSD M.2 |
| Grafika | Komputer w oferowanej konfiguracji musi osiągać w teście wydajności BAPCO SYSmark 25 wynik 1000 pkt. **Wydruk z oprogramowania testującego załączyć do oferty** |
| Klawiatura | Klawiatura odporna na zalanie (układ US), min 100 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo 2x2W.<br>Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy.<br>Kamera internetowa 720p z diodą informującą o aktywności, trwale zainstalowana w obudowie matrycy.<br>1 port audio typu combo (słuchawki i mikrofon) |
| Łączność bezprzewodowa | Wi-Fi 5 ax 2x2 + Bluetooth 5 |
| Bateria i zasilanie | Polimerowa 35 Whr, umożliwiająca szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.<br>Czas pracy na baterii, komputera w oferowanej konfiguracji, musi wynosić 9 godzin, według wyniku testu MobileMark25 Battery Life - **do oferty załączyć wydruk z oprogramowania testującego;**<br>Zasilacz o mocy 65W |
| Waga | Maksymalnie 1,8 kg. z baterią |

| | |
|---|---|
| Obudowa | Szkielet obudowy i zawiasy notebooka wzmacniane;<br>Dookoła matrycy uszczelnienie chroniące klawiaturę po zamknięciu przed kurzem i wilgocią. |
| Certyfikaty | Laptop musi być wyprodukowany zgodnie z normami ISO9001 i ISO50001 – **certyfikaty załączyć do oferty;** |
| Diagnostyka | System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera.<br>Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez: dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, pendrive; |
| Bezpieczeństwo | TPM; |
| Porty i złącza | Wbudowane (nie dopuszcza się przejściówek):<br>1 x HDMI 1.4<br>1 x RJ-45,<br>3 x USB w tym min. 2x USB 3.2;<br>Czytnik kart SD lub microSD<br>port zasilania, złącze linki zabezpieczającej |
| Warunki gwarancyjne | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.<br>3-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego.<br>Oferent musi posiadać ISO 27001 na świadczenie usług – **certyfikat załączyć do oferty** |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>• Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>c) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>d) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych<br>• Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br>• Interfejs użytkownika dostępny w języku polskim i angielskim<br>• Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>• Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe<br>• Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego;<br>• System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,<br>• Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.<br>• Graficzne środowisko instalacji i konfiguracji w języku polskim<br>• Wbudowany system pomocy w języku polskim.<br>• Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).<br>• Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego.<br>• Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. |

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

| | |
|---|---|
| | • Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych;<br>• Możliwość tworzenia wirtualnych kart inteligentnych.<br>• Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)<br>• Wsparcie dla IPSEC oparte na politykach;<br>• Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;<br>• Mechanizmy logowania w oparciu o:<br>a) Login i hasło,<br>b) Karty inteligentne i certyfikaty (smartcard),<br>c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM;<br>• Umozliwiajacy pracę w domenie; |
| Oprogramowanie zabezpieczające | 1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,<br>2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,<br>3. Stosowanie kwarantanny;<br>4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)<br>5. Skanowanie urządzeń USB natychmiast po podłączeniu,<br>6. Automatyczne odłączanie zainfekowanej końcówki od sieci<br>7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.<br>8. Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.<br>9. Musi posiadać moduł ochrony IDS/IPS<br>10. Musi posiadać mechanizm wykrywania skanowania portów<br>11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów<br>12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości<br>13. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH.<br>14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa;<br>15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom.<br>16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa;<br>17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa;<br>18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; |

| | |
|---|---|
| | 19. Blokada możliwości uruchamiania oprogramowania z takich dysków.<br>20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.<br>21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji.<br>22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware.<br>23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.<br>24. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika.<br>25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.<br>26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware;<br>27. Konsola zarządzająca musi umożliwiać co najmniej:<br>a) przechowywanie danych w bazie typu SQL;<br>b) zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory;<br>c) tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi;<br>d) centralna dystrybucja na zarządzanych laptopach uaktualnień definicji ochronnych bez dostępu do sieci Internet.<br>e) raportowanie, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach;<br>f) definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji;<br>28. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych zainstalowanych w różnych lokalizacjach;<br>29. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze;<br>30. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy;<br>31. Musi posiadać dostęp do konsoli z dowolnego miejsca;<br>32. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń<br>33. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej<br>34. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych;<br>35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych;<br>36. Konsola systemu musi umożliwiać, co najmniej:<br>a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie<br>b) przyznanie praw dostępu dla nośników pamięci tj. USB, CD<br>c) regulowanie połączeń WiFi i Bluetooth |

| | |
|---|---|
| | d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe<br>e) blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi<br>f) blokowanie dostępu dowolnemu urządzeniu<br>g) tymczasowe dodania dostępu do urządzenia przez administratora<br>h) szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu;<br>i) zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka<br>j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora<br>k) używanie tylko zaufanych urządzeń sieciowych;<br>37. Wirtualna klawiatury<br>38. Możliwość blokowania każdej aplikacji<br>39. Możliwość zablokowania aplikacji w oparciu o kategorie<br>40. Możliwość dodania własnych aplikacji do listy zablokowanych<br>41. Dodawanie aplikacji w formie portable<br>42. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji<br>43. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool<br>44. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.<br>45. Możliwość zablokowania funkcji Printscreen<br>46. Monitorowania przesyłu danych między aplikacjami;<br>47. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików<br>48. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj<br>49. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe<br>50. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe<br>51. Ochrona zawartości schowka systemu<br>52. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL<br>53. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych<br>54. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem<br>55. Możliwość tworzenia profilu DLP dla każdej polityki<br>56. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania<br>57. Ochrona przez wyciekiem plików poprzez programy typu p2p<br>58. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.<br>59. Monitorowanie określonych rodzajów plików.<br>60. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.<br>61. Możliwość śledzenia zmian we wszystkich plikach |

| | |
|---|---|
| | 62. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach;<br>63. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku<br>64. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich<br>65. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email<br>66. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika<br>67. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi<br>68. Musi posiadać możliwość eksportu danych użytkownika<br>69. Musi umożliwiać import listy urządzeń z pliku CSV<br>70. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych<br>71. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta;<br>72. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora;<br>73. Musi zawierać podgląd aktualnie zainstalowanych aplikacji<br>74. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,<br>75. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł<br>76. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres<br>77. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa:<br>78. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową<br>79. Portal musi być dostępny w postaci usługi hostowanej;<br>80. Skanowanie podatności za pomocą nodów skanujących<br>81. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie<br>82. Portal zarządzający musi umożliwiać:<br>a) przegląd wybranych danych na podstawie konfigurowalnych widgetów<br>b) zablokowanie możliwości zmiany widgetów<br>c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.<br>d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności<br>e) eksport wszystkich skanów podatności do pliku CSV;<br>84. Backup i przywracanie danych;<br>85. Deduplikacja danych na źródle,<br>86. Backup przyrostowy i różnicowy,<br>87. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,<br>88. Backup danych lokalnych – plikowy oraz poczty;<br>89. Backup otwartych plików;<br>90. Filtr plików oraz folderów;<br>91. Domyślne wykluczenia zbędnych plików; |

| | |
|---|---|
| | 92. Przywracanie danych do wskazanej lokalizacji,<br>93. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora;<br>94. Wyszukiwanie plików w repozytorium użytkownika;<br>95. Automatyczne logowanie;<br>96. Zapamiętywanie danych logowania;<br>97. Automatyczne uruchamianie programu przy starcie systemu;<br>98. Ustawianie priorytetu dla procesu backupu;<br>99. Zmiana klucza szyfrującego;<br>100. Ustawienia przepustowości/zajętości pasm;,<br>101. Konfiguracja wydajności procesu backup;<br>102. Zastępowanie nazwy pliku GUID-em;<br>103. Szyfrowanie danych algorytmem AES 256 CBC po stronie komputera użytkownika,<br>104. Kompresja danych;<br>105. Transmisja po bezpiecznym protokole TLS;<br>106. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji;<br>107. Obliczanie sumy kontrolnej;<br>108. Kopie zapasowe musza być przechowywane w data center;<br>109. Licencje przypisywane do urządzenia z przestrzenią w chmurze 50 GB.<br>110. Licencja obowiązuje minimum przez okres gwarancji laptopa.<br>111. Wsparcie techniczne musi być świadczone w języku polskim; |

## VI. Zestaw do nauki hybrydowej – 8 szt.

1. Założenie ogólne:
   - 1.1 Zestaw USB umożliwiający wykorzystanie z dowolną platformą do wideokonferencji takimi jak np. Microsoft Teams, Zoom, Google Meet Workspace, Cisco Webex itp
   - 1.2 Zestaw modularny, elementy zestawu takie jak kamera, głośnik oraz mikrofony muszą być zasilone z jednego centralnego punktu
     - 1.2.1 Kamery i głośniki z centralnego urządzenia zamontowanego za monitorem;
     - 1.2.2 Mikrofony z drugiego centralnego urządzania zamontowanego pod stołem konferencyjnym
     - 1.2.3 Między urządzeniem centralnym, zamontowanym za monitorami i pod stołem może być poprowadzony tylko jeden przewód tj: skrętka kategorii CAT6A
2. Kamera – 1 sztuka
   - 2.1 Kamera PTZ 4K 30kl/s
   - 2.2 Zoom optyczny - 5x
   - 2.3 Zakres widzenia w poziomie – 80 stopni
   - 2.4 Pole widzenia po przekątnej - 90stopni
   - 2.5 Zakres ruchu kamery w poziomie - +/- 80 stopni
   - 2.6 Zakres ruchu kamery w pionie – 40 stopni / - 90 stopni
   - 2.7 Autofocus
   - 2.8 Możliwość ustawienia 3 predefiniowanych widoków kamery
   - 2.9 Możliwość automatycznego kadrowania grupy osób w sali
   - 2.10 Tryb uśpienia kamery, tryb prywatności – automatyczne pochylenie kamery o -90 stopni gdy nie ma połączenia wideo oraz po zakończeniu spotkania
   - 2.11 Slot do zabezpieczenia kamery – Kensington
3. Kamera zawartości USB:
   - 3.1 Kamera zawartości kompatybilna z dowolnym komputerem
   - 3.2 Kamera musi umożliwiać wysłanie treści z tablicy sucho ścieralnej zainstalowanej w sali wykładowej;

3.3 Kamera musi zapewniać. efekt przejrzystości tzn. pokazywać tylko to co jest na tablicy, a osoba pisząca musi być transparentna;
3.4 Kamera musi poprawiać kontrast i kolor pisaków sucho ścieralnych
3.5 Kamera musi być zasilana z PoE
3.6 Kamera umożliwiająca centralne zarządzanie z poziomu panelu do zarządzania
3.7 Wraz z kamerą muszą być dostarczone wszystkie niezbędne elementy montażowe do przymocowania kamery nad tablicą sucho ścieralną oraz okablowanie;

4. Mikrofon – 2 sztuki
   4.1 Zakres pracy mikrofonów – strefa o promieniu 2 metrów
   4.2 Technologia kształtowania wiązki tzw „beamforming" tj. mikrofon musi skupiać się na dźwięku osoby mówiącej
   4.3 Wbudowane technologie akustyczne: AEC, aktywne wykrywanie osoby mówiącej oraz eliminacja szumów otoczenia
   4.4 Możliwość instalacji kaskady 4 mikrofonów;
   4.5 Połączenie mikrofonu - szeregowe lub topologia gwiazdy
   4.6 Przycisk wycieszenia mikrofonu wraz ze podświetleniem statusu pracy;
5. Głośnik – 2 sztuki
6. Okablowanie oraz zestaw montażowy;
7. Stacja dokująca z funkcją Power PassThrough pozwalająca na dodanie 10 urządzeń z przejściem zasilania, przy pomocy 1 kabla;

| Nazwa komponentu | Wymagane minimalne parametry techniczne |
|---|---|
| Porty USB | 3 x USB 3.1 Gen1 o łącznej mocy wyjściowej 10 W; |
| Wyjście wideo | 1 x DisplayPort, 1 x HDMI, 1 x VGA |
| Porty LAN | 1 x złącze Gigabit Ethernet |
| Audio | 1 x 3,5 mm mikrofon i gniazdo słuchawkowe |
| Zasilanie | 1 x USB-C |
| Pamięć flash | 1 x gniazdo kart SD/SDHC/SDXC<br>1 x gniazdo kart Micro SD/SDHC/SDXC z obsługą kart 128 GB; |
| Rozdzielczość wideo | DisplayPort — 3840 x 2160@30<br>HDMI — 3840 x 2160@30<br>VGA — 1920 x 1200@60 |
| Pobór mocy | Maksymalnie 15WBTU |
| Obudowa | Aluminium |

8. Z zestawem powinny być dostarczone kompletne okablowanie umożliwiające prawidłowe połączenie urządzeń oraz montaż całości w lokalizacjach wskazanych przez zamawiającego;

Gwarancja na cały zestaw – 24 miesiące

## VII. Szkolenie on-line dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania – 62 szt.

**1. Przedmiot zamówienia**

Szkolenie on-line dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania. Przygotowanie i przeprowadzenie szkolenia online w czasie rzeczywistym dla pracowników Zamawiającego.

**2. Zakres merytoryczny szkolenia**

Główny cel szkolenia nabycie wiedzy i umiejętności pracowników Zamawiającego z zakresu obsługi zakupionego sprzętu i oprogramowania.

**3. Czas trwania szkolenia:** 1 dzień (6 godzin) dla każdego uczestnka.

**4. Forma szkolenia -** online w czasie rzeczywistym z zapisem cyfrowym szkolenia umożliwiającym jego późniejsze odtworzenie. Wykonawca przekaże Zamawiającemu kopię elektroniczną zarejestrowanego szkolenia na nośniku elektronicznym.

**5. Materiały szkoleniowe** dla uczestników, w formie PDF lub prezentacji PowerPoint.

**6. Zaświadczenia ukończenia szkolenia.**

- zostaną przygotowane zgodnie z wytycznymi Zamawiającego na podstawie przesłanych list uczestników biorących udział w szkoleniu;
- będą zawierały imię i nazwisko uczestnika, tytuł wskazujący na realizowany program szkolenia, informację o terminie jego przeprowadzenia oraz liczbę godzin szkoleniowych;

**7. Wsparcie poszkoleniowe trenera**

Wykonawca zapewni uczestnikom dodatkowy 14-dniowy kontakt telefoniczny z trenerem po szkoleniu w godzinach 8.00-15.00.

**8. OPIS SZKOLENIA**

a) Zaznajomienie uczestników z zasadami obsługi poszczególnych sprzętów i oprogramowania zakupionych w postępowaniu,
b) Przedstawienie zasad BHP przy użytkowaniu sprzętów i oprogramowania,
c) Zaznajomienie uczestników z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem, a także w jaki sposób zabezpieczać się przed takimi atakami i groźbą utraty danych,
d) Podczas szkolenia przedstawione zostaną ryzyka wykorzystywania komputera służbowego do celów prywatnych;
e) Szkolenie musi być dostosowane do każdego pracownika bez względu na jego wiedzę i umiejętności informatyczne.
f) Szkolenie umożliwi zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi.

**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.**