Zadanie realizowane jest w zakresie umowy o powierzenie grantu o numerze 4914/3/2022 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" o numerze POPC.05.01.00-00-0001/21-00

Projekt „Cyfrowa gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2020.

Nazwa postępowania:

Zakup sprzętu komputerowego oraz oprogramowania na potrzeby projektu "Cyfrowa Gmina".

OPIS PRZEDMIOTU ZAMÓWIENIA

Część I Sprzęt

1) Zasilacz awaryjny do serwerowni.

Zasilacz awaryjny do serwerowni. Szczegółowy opis:

Zakup i dostawa fabrycznie nowego zasilacza awaryjnego UPS z przeznaczeniem do szafy serwerowej.

Opis parametrów:

a) gwarancja: 24 miesięczna gwarancja producenta na urządzenie
b) obudowa: możliwość montażu w szafie rack, urządzenie dostarczana z kompletem elementów montażowych
c) Moc wyjściowa pozorna: 3000 VA lub więcej
d) Moc wyjściowa czynna: 2700 W lub więcej
e) Zakres napięcia wyjściowego: 230 V (+6/–10 %)
f) Kształt napięcia wyjściowego: sinosuidalny
g) Rodzaj gniazd 8 x IEC-320-C13, 1 x IEC-320-C19 lub więcej
h) Interfejs: USB
i) Wyświetlacz pokazujące najważniejsze parametry urządzenia

2) Modernizacja kopii zapasowej

Przedmiot zamówienia obejmuje dostawę sprzętu wraz z konfiguracją według wskazań administratora. W ramach tej pozycji wymagana jest dostawa sieciowego serwera plików wraz dyskami twardymi, ich montażem oraz licencjami oprogramowania do wykonywania kopii bezpieczeństwa.

Lp.	Nazwa parametru	Minimalna wartość parametru
1.	Sieciowy serwer plików w obudowie typu	Sieciowy serwer plików – 1 szt.: • Obudowa typu rack 1U • Procesor czterordzeniowy o taktowaniu co najmniej 2.0

	rack.	Ghz • Pamięć RAM 4 GB lub większa SODIMM DDR4 • Obudowa umożliwiająca montaż czterech dysków twardych • Kontroler RAID 0,1,10,5,6 • Dwie karty sieciowe 10/100/1000/2500 MBit/s • Dodatkowe złącza HDMI, 2 x USB 2.0, 2xRJ-45, 2x USB 3.1 • Gniazdo rozszerzeń 1x PCIe 2.0 x2 • Gwarancja 36 miesięcy Zainstalowane cztery dyski twarde o łącznej pojemności co najmniej 24 TB przystosowane do ciągłej pracy w serwerach NAS • Interfejs dysku SATA III – 6 Gb/s • Prędkość obrotowa dysku 5400 RPM • Pamięć podręczna 128MB • Pojemność każdego dysku co najmniej 6 TB • Ochrona przed zakłóceniami i drganiami • Gwarancja 36 miesięcy
2.	Oprogramowanie do wykonywania kopii bezpieczeństwa	Opis przedmiotu zamówienia: dostawa licencji profesjonalnego oprogramowania do wykonywania kopi zapasowych o parametrach równych lub wyższych: a) oprogramowanie pozwalające na wykonywanie kopii zapasowych z jednego hypervisora bez limitu maszyn wirtualnych oraz minimum dwóch systemów serwerowych w sposób pozwalający wykonać kopie zasobów znajdujących się na tych systemach. b) minimalne funkcjonalności: wykonywanie kopii zapasowych całych dysków twardych wraz z działającym systemem operacyjnym, szyfrowanie kopii zapasowych algorytmem szyfrujących AES 256, odzyskiwanie całego systemu operacyjnego na ten sam lub inny sprzęt komputerowy, odzyskiwanie poszczególnych folderów i plików, weryfikowanie kopii zapasowych, kompresowanie kopii zapasowych, funkcjonalność replikacji kopii zapasowych, weryfikacja kopii zapasowych, ochrona kopii zapasowych przed działaniem ransomware. c) metody wykonywania kopii zapasowych: pełna, przyrostowa, różnicowa lub więcej, c) oprogramowanie musi posiadać konsolę administracyjną z funkcjonalnością nie niższą niż: powiadomienia e-mail o zdarzeniach, podgląd wykonywania

		kopii zapasowych, logi, harmonogram wykonywania kopii, odzyskiwanie kopii zapasowych,
3.	Wdrożenie	Wdrożenie powinno obejmować następujące elementy: • Dostawę dysku sieciowego NAS wraz z instalacją dysków twardych oraz oprogramowania potrzebnego do funkcjonowania NAS • Instalacja oprogramowania do wykonywania kopii bezpieczeństwa według wytycznych administratora systemu na wskazanym przez niego systemie. • Konfigurację zadań backupu według wytycznych administratora systemu (maksymalnie 8 zadań).

3) Urządzenie do ochrony sieci

Dostawa urządzenia klasy UTM wraz z wdrożeniem

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. W ramach posiadanej licencji urządzenie ma umożliwiać skorzystanie z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
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.
94. Urządzenie ma być objęte gwarancją typu NBD tzn. w przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od potwierdzenia awarii.

PARAMETRY SPRZĘTOWE

95. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
96. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
97. Liczba portów Ethernet 10/100/1000Mbps – min.8.
98. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
99. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
100. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2.4Gbps.
101. Przepustowość filtrowania Antywirusowego – minimum 495Mbps.
102. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 600Mbps.
103. Maksymalna liczba tuneli VPN IPSec – minimum 100.
104. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
105. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
106. Obsługa interfejsów 802.11q (VLAN) – minimum 128
107. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 18 000 nowych sesji/sekundę.
108. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
109. Urządzenie nie ma limitu na liczbę użytkowników.
110. Liczba reguł filtrowania – minimum 8 192.
111. Liczba tras statycznego routingu – minimum 512.
112. Liczba tras dynamicznego routingu – minimum 10 000.

WDROŻENIE

113. Wykonawca dostarczy i zainstaluje urządzenie UTM we wskazanym miejscu w lokalizacji Zamawiającego, w siedzibie Urzędu Gminy
114. Dostarczony sprzęt musi być fabrycznie nowy i oryginalnie zapakowany.
115. Wykonawca przeprowadzi wdrożenie dostarczonego urządzenia UTM zastępując nim obecnie pracujące urządzenie Zamawiającego. Konfiguracja obecnego urządzenia składa się z następujących elementów:
    - Zmiana domyślnych haseł,
    - Zmiana strefy czasowej i ustawienie poprawnej daty/godziny,
    - Rejestracja urządzenia na stronie producenta,
    - Aktualizacja oprogramowania (jeśli jest konieczna),

- Konfiguracja DHCP
- Konfiguracja profili bezpieczeństwa (IPS),
- Konfiguracja do 4 portów LAN/WAN,
- W ramach konfiguracji 4 portów LAN/WAN konfiguracja QOS lub failover / load balancing'u (jeśli jest konieczna, bez konfiguracji routingu dynamicznego np. BGP),
- Konfiguracja do 20 reguł bezpieczeństwa (reguł firewall),
- Konfiguracja do 5 reguł NAT,
- Utworzenie obiektów według wytycznych administratora,
- Konfiguracja SSL VPN Client To Site dla co najmniej 10 użytkowników,
- Konfiguracja 1 tunelu VPN Site To Site (jeśli jest konieczna),
- Konfiguracja urządzenia w trybie routera (NAT) lub w trybie transparentnym (bez konfiguracji usług zewnętrznych np. innych urządzeń sieciowych lub urządzeń zależnych),
- Konfiguracja połączenia z AD (integracja) lub utworzenie lokalnej bazy LDAP,
- Stworzenie reguł URL filtering'u według wytycznych administratora.

Konfiguracja urządzenia w celu zapisywania logów na karcie pamięci lub zewnętrznym serwerze logów

4) zestaw PC – PC+ monitor

Zakup i dostawa fabrycznie nowych pięciu zestawów komputerowych o następujących parametrach:

a) Komputer stacjonarny:
- Producent: dowolny,
- obudowa wolno stojąca, niezintegrowana z monitorem,
- gwarancja: 36 miesięczna gwarancja producenta,
- pamięć RAM: 8 GB lub więcej,
- procesor: 1 jednostka CPU, 6 rdzeni fizycznych lub więcej, o taktowaniu bazowym minimum 2,8 Ghz lub równoważnym czyli osiągający nie mniej niż 12 000 punktów (CPU Mark) w teście https://www.cpubenchmark.net/
- dysk twardy: pojemność minimum 240 GB, prędkość odczytu/zapisu danych minimum 450 MBps,
- karta graficzna: dedykowana przez producenta zapewniająca prawidłową pracę,
- płyta główna: dedykowana przez producenta zapewniająca prawidłową pracę, wbudowany moduł TPM 2.0,
- złącza IO: minimum 1xHDMI, 1xRJ45 100/1000 Mbit/s, (panel tylny) 4xUSB, audio, (panel przedni) 2xUSB,
- peryferia: dedykowane przez producenta myszka komputerowa, pełnowymiarowa klawiatura QWERTY,

- System operacyjny, zainstalowany w najnowszej dostępnej wersji, na urządzeniu powinien być wyposażony w oprogramowanie antywirusowe z bezpłatną aktualizacją sygnatur. Urządzenie musi posiadać dedykowaną partycję „recovery" umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. W przypadku braku partycji „recovery" do komputera wymagany jest nośnik zewnętrzny umożliwiający odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii lub oprogramowanie producenta komputera umożliwiające utworzenie takiego nośnika. Klucz licencyjny systemu operacyjnego, może być zapisany trwale w BIOS lub dostarczony jako naklejka licencyjna umieszczona na

obudowie komputera. System operacyjny musi umożliwiać pełną 100% współpracę z Microsoft Active Directory oraz pozwalać na instalację następującego oprogramowania: System operacyjny musi umożliwiać bezpośrednie (bez np. emulatorów) zainstalowanie i używanie następujących aplikacji: Microsoft Teams, Microsoft Office, Axence nVision, FerroBackup.)

b) Monitor:
- gwarancja: 24 miesięczna gwarancja producenta lub dłuższa
- przekątna ekranu: około 24 cale
- typ ekranu: płaski, dedykowany do pracy biurowej
- rozdzielczość nominalna: 1920x1080
- typ matrycy: matryca o kącie widzenia w pionie i poziomie 178 stopni lub więcej,
- powłoka matrycy: matowa, antyrefleksyjna
- wbudowane głośniki
- możliwość regulacji: pochył, wysokość
- ochrona oczu: redukcja migotania, filtr światła niebieskiego
- złącza portów video: HDMI, Display Port lub więcej
- porty wyjścia\wejścia: USB
- klasa energetyczna: E lub o niższym użyciu energii zgodnie z oznaczeniami obowiązującymi od 1 marca 2021 roku

5) Jednostki PC - 2 szt.

Zakup i dostawa fabrycznie nowych dwóch komputerów PC o następujących parametrach:

a) Komputer stacjonarny:
- Producent: dowolny,
- obudowa wolno stojąca, niezintegrowana z monitorem,
- gwarancja: 36 miesięczna gwarancja producenta,
- pamięć RAM: 8 GB lub więcej,
- procesor: 1 jednostka CPU, 6 rdzeni fizycznych lub więcej, o taktowaniu bazowym minimum 2,8 Ghz lub równoważnym czyli osiągający nie mniej niż 12 000 punktów (CPU Mark) w teście https://www.cpubenchmark.net/
- dysk twardy: pojemność minimum 240 GB, prędkość odczytu/zapisu danych minimum 450 MBps,
- karta graficzna: dedykowana przez producenta zapewniająca prawidłową pracę,
- płyta główna: dedykowana przez producenta zapewniająca prawidłową pracę, wbudowany moduł TPM 2.0,
- złącza IO: minimum 1xHDMI, 1xRJ45 100/1000 Mbit/s, (panel tylny) 4xUSB, audio, (panel przedni) 2xUSB,
- peryferia: dedykowane przez producenta myszka komputerowa, pełnowymiarowa klawiatura QWERTY,

- System operacyjny, zainstalowany w najnowszej dostępnej wersji, na urządzeniu powinien być wyposażony w oprogramowanie antywirusowe z bezpłatną aktualizacją sygnatur. Urządzenie musi posiadać dedykowaną partycję

„recovery” umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. W przypadku braku partycji „recovery” do komputera wymagany jest nośnik zewnętrzny umożliwiający odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii lub oprogramowanie producenta komputera umożliwiające utworzenie takiego nośnika. Klucz licencyjny systemu operacyjnego, może być zapisany trwale w BIOS lub dostarczony jako naklejka licencyjna umieszczona na obudowie komputera. System operacyjny musi umożliwiać pełną 100% współpracę z Microsoft Active Directory oraz pozwalać na instalację następującego oprogramowania: System operacyjny musi umożliwiać bezpośrednie (bez np. emulatorów) zainstalowanie i używanie następujących aplikacji: Microsoft Teams, Microsoft Office, Axence nVision, FerroBackup.)

6) Serwer dla jednostek podległych 2 szt.

Zakup i dostawa dwóch w pełni funkcjonalnych fabrycznie nowych serwerów z systemem operacyjnym i licencjami dostępowymi. Parametry:

a) Obudowa: typ tower
b) Procesor: 1 jednostka CPU, 4 rdzeni fizycznych, o taktowaniu bazowym minimum 2,8 Ghz lub równoważnym, osiągający nie mniej niż 8 000 punktów (CPU Mark) w teście https://www.cpubenchmark.net/
c) Pamięć RAM: dedykowana przez producenta nie mniej niż 16GB,
d) Dyski twarde: minimum 2x960GB, o prędkościach odczyt/zapis minimum 54 0 MB/s 520 MB/s, dedykowany do pracy mieszanej(zapis/odczyt), bez podzespołów mechanicznych. Dodatkowy dysk twardy SATA o pojemności minimum 2 TB
e) Kontroler RAID sprzętowy
f) Napęd optyczny: DVD-RW
g) Karty sieciowe: minimum 2xRJ45, 1GbE,
h) Zdalne zarządzanie: poprzez sieć komputerową za pośrednictwem RJ-45
i) Gwarancja producenta: minimum 3 lata typu Next Business Day (naprawa/wymiana u klienta, czas reakcji następny dzień roboczy)
j) Licencja na system operacyjny
   -Typ licencji: komercyjna,
   -Rodzaj licencji: nowa licencja,
   -Okres licencji: wieczysta. Architektura: 64 bit,
   -Wersja językowa: polska,
   -Klasa produktu: system operacyjny,
   -Łączna suma rdzeni procesorów w serwerze nie może przekraczać 10
   - Max 64GB pamięci ram
   - Max liczna licencji CAL 25 użytkowników i 50 urządzeń (nie ma konieczności ich dokupowania)
   - Brak możliwości instalacji licencji CAL RDS
   -Praca w roli serwera domeny Active Directory
   -Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP)
   -Zawarta możliwość uruchomienia roli serwera DNS

-Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP)
-Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Active Directory
-Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Active Directory
-Zawarta możliwość uruchomienia roli serwera stron WWW
Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
- Klucz licencyjny systemu operacyjnego, może być zapisany trwale w BIOS lub dostarczony jako naklejka licencyjna umieszczona na obudowie jednostki
- Obecnie aplikacje dziedzinowe wykorzystują silnik baz danych MSSQL

7) Zakup rozwiązań do kopii bezpieczeństwa i zasilaczy awaryjnych UPS dla podległych jednostek

7.1.Zakup i dostawa dwóch fabrycznie nowych urządzeń do archiwizacji NAS Desktop.
Parametry:

a) Obudowa: typ tower
b) Procesor: 1 jednostka CPU, 4 rdzenie fizyczne, o taktowaniu bazowym minimum 2,0 Ghz lub równoważnym czyli osiągający nie mniej niż 2800 punktów (CPU Mark) w teście https://www.cpubenchmark.net/cpu_list.php
c) Pamięć RAM: dedykowana przez producenta nie mniej niż 8 GB,
d) Wbudowana pamięć flash: min: 4 GB
e) Dyski twarde: minimum 2x4TB Hot-Plug, o przepustowości min. 6Gb/s, dedykowany do pracy mieszanej(zapis/odczyt)
f) Kontroler RAID

Poziomy RAID
- 0
- 1
- 10 (1+0)
- 5
- 50 (5+0)
- 6
- JBOD

g) Zasilanie: dwa zasilacze redundantne, hot-plug, o mocy 750W lub więcej,
h) Karty sieciowe: minimum 2xRJ45 10/100/1000/2500 Mbit/s
i) Gniazda we/wy: 1xHDMI, 3 x USB 2.0, 2xUSB 3.0,
j) Gniazda rozszerzeń: 1 x PCIe 2.0 x 2
k) Zasilanie: 120 W
l) Liczba wentylatorów :min 2 sztuki
m) Gwarancja producenta: minimum 2 lat typu

7.2.Zakup i dostawa fabrycznie nowych dwóch dysków twardych HDD Parametry:

a) Tup dyski : HDD
b) Format szerokości : 3,5'' (LFF)
c) Pojemność dysku : min 4 TB
d) Interfejs dysku : SATA
e) Prędkość obrotowa: min 5400 obr/min
f) Bufor: min 256 MB

7.3. Zakup i dostawa fabrycznie nowych dwóch zasilaczy awaryjnych UPS o następujących parametrach:

a) urządzenie zapewniające filtrowania zasilania i podtrzymanie z akumulatora zasilania w przypadku braku zasilania z sieci elektrycznej
b) przeznaczenie: sprzęt komputerowy
c) gwarancja: 24 miesięczna gwarancja producenta na urządzenie
d) obudowa: wolnostojąca
e) Porty zasilania we: IEC-C14
f) Porty zasilania wy: 4 x IEC-C13
g) Gniazda we/wy: 1 x USB (type B), 1 x RS-232 (COM)
h) Funkcje specjalne: Awaryjne wyłączenie EPO
i) Moc wyjściowa pozorna: 800Va lub więcej
j) Moc wyjściowa czynna: 700 W lub więcej
k) Poziom hałasu : 45 dB
l) Zakres napięcia wyjściowego: 220 - 240 V
m) Sygnalizacja: diody/dźwiękowa
n) Oprogramowanie: udostępnione przez producenta oprogramowanie do obsługi urządzenia

8) Zakup Laptopów 4 szt

8.1. **Komputery przenośne Typ I. Szczegółowy opis:**

Zakup i dostawa dwóch fabrycznie nowych przenośnych komputerów z głównym przeznaczeniem do pracy zdalnej. Parametry:

a) Producent: dowolny, legalnie działający na terenie Rzeczpospolitej Polskiej
b) Gwarancja: minimum 24 miesięczna gwarancja producenta urządzenia
c) Dedykowana linia urządzenia: biznesowa
d) Przekątna ekranu: 15,6 cali
e) Rozdzielczość: 1920 x 1080 pikseli (Full HD) lub większa
f) Procesor: wyposażony w cztery fizyczne rdzenie lub więcej, bazowa częstotliwość pracy nie mniej niż 2,3GHz lub równoważny czyli osiągający nie mniej niż 990 punktów (Overall) w teście SYSmark25 Notebook według rankingu: https://results.bapco.com/charts/facet/SYSmark_25/cpu/all/notebook
g) Pamięć RAM: dedykowana przez producenta laptopa o pojemności minimum 16 GB
h) Typ matrycy: dedykowana przez producenta laptopa, matowa lub z powłoką antyrefleksyjną
i) Dysk twardy: pojemność minimum 500 GB, prędkość odczytu/zapisu danych minimum 450 MBps
j) Klawiatura: dedykowana przez producenta laptopa, wbudowana w urządzenie z wydzieloną klawiatura numeryczną, klawiatura obsługująca polski język (programisty, QWERTY)
k) Touchpad: dedykowany przez producenta laptopa, wbudowany w urządzenie
l) Płyta główna: dedykowana przez producenta laptopa płyta główna wyposażone w układy i elementy
niezbędne do prawidłowej pracy, moduł TPM 2.0 lub nowszy
m) Karta graficzna dedykowana przez producenta laptopa, umożliwiająca prawidłową pracę urządzenia
n) Karta dźwiękowa: dedykowana przez producenta laptopa, umożliwiająca prawidłową pracę urządzenia

o) Złącza wejścia/wyjścia IO: minimalna ilość wbudowanych złącz i wyjść IO (Zamawiający dopuszcza, aby laptopy były wyposażone w większą ilość złącz lub innego typu niż minimalnie określona): 1xHDMI, łącznie 3xUSB, WiFi, bluetooth, głośniki, mikrofon, kamera,
p) Zasilanie: Fabryczny zasilacz, dedykowany przez producenta, wbudowana dedykowana bateria
q) System operacyjny, zainstalowany w najnowszej dostępnej wersji, na urządzeniu powinien być wyposażony w oprogramowanie antywirusowe z bezpłatną aktualizacją sygnatur. Urządzenie musi posiadać dedykowaną partycję „recovery" umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. W przypadku braku partycji „recovery" do komputera wymagany jest nośnik zewnętrzny umożliwiający odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii lub oprogramowanie producenta komputera umożliwiające utworzenie takiego nośnika. Klucz licencyjny systemu operacyjnego, może być zapisany trwale w BIOS lub dostarczony jako naklejka licencyjna umieszczona na obudowie komputera. System operacyjny musi umożliwiać pełną 100% współpracę z Microsoft Active Directory oraz pozwalać na instalację następującego oprogramowania: System operacyjny musi umożliwiać bezpośrednie (bez np. emulatorów) zainstalowanie i używanie następujących aplikacji: Microsoft Teams, Microsoft Office, Axence nVision, FerroBackup.)
r) Sterowniki Laptop winien mieć zainstalowane wszystkie sterowniki, zapewniające prawidłowe działanie urządzenia
s) Zabezpieczenia System operacyjny zainstalowany na urządzeniu powinien być wyposażony w oprogramowanie antywirusowe z bezpłatną aktualizacją sygnatur. Urządzenie musi posiadać dedykowaną partycję „recovery" umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. W przypadku braku partycji „recovery" do komputera wymagany jest nośnik zewnętrzny umożliwiający odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii lub oprogramowanie producenta komputera umożliwiające utworzenie takiego nośnika.

Kolor obudowy: czarny, srebrny, czarno-srebrny

8.2. **Komputer przenośny Typ II. Szczegółowy opis:**

Zakup i dostawa dwóch fabrycznie nowego przenośnego komputera z głównym przeznaczeniem do pracy zdalnej i serwisowania infrastruktury IT. Parametry:

t) Producent: dowolny, legalnie działający na terenie Rzeczpospolitej Polskiej
u) Gwarancja: minimum 24 miesięczna gwarancja producenta urządzenia
v) Dedykowana linia urządzenia: biznesowa
w) Przekątna ekranu: 15,6 cali
x) Rozdzielczość: 1920 x 1080 pikseli (Full HD) lub większa
y) Procesor: wyposażony w cztery fizyczne rdzenie lub więcej, bazowa częstotliwość pracy nie mniej niż 2,2GHz lub równoważny czyli osiągający nie mniej niż 1 300 punktów (Overall) w teście SYSmark25 Notebook według rankingu: https://results.bapco.com/charts/facet/SYSmark_25/cpu/all/notebook
z) Pamięć RAM: dedykowana przez producenta laptopa o pojemności minimum 8 GB
aa) Typ matrycy: dedykowana przez producenta laptopa, matowa lub z powłoką antyrefleksyjną
bb) Dysk twardy: pojemność minimum 500 GB, prędkość odczytu/zapisu danych minimum 500 MBps
cc) Klawiatura: dedykowana przez producenta laptopa, wbudowana w urządzenie, klawiatura obsługująca polski język (programisty, QWERTY)
dd) Touchpad: dedykowany przez producenta laptopa, wbudowany w urządzenie
ee) Płyta główna: dedykowana przez producenta laptopa płyta główna wyposażone w

układy i elementy niezbędne do prawidłowej pracy, moduł TPM 2.0 lub nowszy

ff) Karta graficzna dedykowana przez producenta laptopa, umożliwiająca prawidłową pracę urządzenia

gg) Karta dźwiękowa dedykowana przez producenta laptopa, umożliwiająca prawidłową pracę urządzenia

hh) Złącza wejścia/wyjścia IO minimalna ilość wbudowanych złącz i wyjść IO (Zamawiający dopuszcza, aby laptopy były wyposażone w większą ilość złącz lub innego typu niż minimalnie określona): 1xHDMI, łącznie 3xUSB (w tym min. 1 Typ-C), WiFi, bluetooth, głośniki, mikrofon, kamera,

ii) Zasilanie Fabryczny zasilacz, dedykowany przez producenta, wbudowana dedykowana bateria

jj) System operacyjny, zainstalowany w najnowszej dostępnej wersji, na urządzeniu powinien być wyposażony w oprogramowanie antywirusowe z bezpłatną aktualizacją sygnatur. Urządzenie musi posiadać dedykowaną partycję „recovery" umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. W przypadku braku partycji „recovery" do komputera wymagany jest nośnik zewnętrzny umożliwiający odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii lub oprogramowanie producenta komputera umożliwiające utworzenie takiego nośnika. Klucz licencyjny systemu operacyjnego, może być zapisany trwale w BIOS lub dostarczony jako naklejka licencyjna umieszczona na obudowie komputera. System operacyjny musi umożliwiać pełną 100% współpracę z Microsoft Active Directory oraz pozwalać na instalację następującego oprogramowania: System operacyjny musi umożliwiać bezpośrednie (bez np. emulatorów) zainstalowanie i używanie następujących aplikacji: Microsoft Teams, Microsoft Office, Axence nVision, FerroBackup.)

kk) Sterowniki Laptop winien mieć zainstalowane wszystkie sterowniki, zapewniające prawidłowe działanie urządzenia

ll) Zabezpieczenia System operacyjny zainstalowany na urządzeniu powinien być wyposażony w oprogramowanie antywirusowe z bezpłatną aktualizacją sygnatur. Urządzenie musi posiadać dedykowaną partycję „recovery" umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. W przypadku braku partycji „recovery" do komputera wymagany jest nośnik zewnętrzny umożliwiający odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii lub oprogramowanie producenta komputera umożliwiające utworzenie takiego nośnika.

Część II: Oprogramowanie

1) Chmura Obliczeniowa JST

Utworzenie chmury prywatnej do przechowywania kopii zapasowych. Szczegółowy opis:
Zakup licencji - usługi wykonywania kopii w chmurze -300 GB

Lp.	Nazwa parametru	Minimalna wartość parametru
1.	Rozwiązanie do wykonywania kopii bezpieczeństwa w chmurze	Rozwiązanie do wykonywania kopii bezpieczeństwa w chmurze składające o wymienionej funkcjonalności lub równoważnej. **INSTALATOR** Instalator umożliwia zainstalowanie aplikacji klienckiej na komputerze użytkownika końcowego. Na instalator składają się następujące funkcje: ● Kreator instalacji,

		● Tłumaczenie instalatora na inne języki, ● Automatyczna instalacja dodatkowych komponentów. **APLIKACJA WINDOWS** Część kliencka powinna składać się z dwóch elementów, aplikacji klienckiej oraz usługi systemowej. Aplikacja kliencka instalowana na komputerze użytkownika końcowego powinna być odpowiedzialna za konfigurację i administrację politykami backupu. Usługa systemowa powinna stanowić właściwy silnik backupu i być odpowiedzialna za wykonywanie backupów oraz synchronizację danych. Aplikacja kliencka nie musi być uruchomiana dla prawidłowego działania usługi. Rozwiązanie powinno umożliwiać Backup i przywracanie danych w następujący sposób: ● Deduplikacja danych na źródle, ● Backup przyrostowy Delta, ● Backup różnicowy Delta, ● Bare Metal Recovery, ● Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, ● Retencja danych ● Kreator projektów backupów - polityka backupu, ● Projekty backupów, ● Backup danych lokalnych - plikowy, ● Backup MS Outlook, ● Backup MS SQL, ● Backup Firebird, ● Backup dysków sieciowych, ● Backup MS Exchange ● Backup MySQL, ● Backup PostgreSQL, ● Backup System State, ● Backup Hyper-V, ● Backup VMware, ● Backup VMware dla darmowych licencji, ● Windows Operating System Backup – VHD, ● Backup z wykorzystaniem skryptów pre i post, ● Backup obrazu dysku, ● Harmonogramy backupów, ● Backup otwartych plików (VSS), ● Filtr plików oraz folderów, ● Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), ● Wyłączanie komputera po wykonaniu backupu,

		● Backup na prawach użytkownika systemu Windows, ● Backup na prawach użytkownika AD, ● Przywracanie danych do wskazanego katalogu, ● Przywracanie danych do pierwotnej lokalizacji, ● Przywracanie wybranej wersji pliku, ● Możliwość backup-u z wykorzystaniem wielu rdzeni procesora, ● Możliwość przywracania z wykorzystaniem wielu rdzeni procesora, ● Przywracanie plików z określonego hosta, ● Przywracanie plików z określonego projektu, ● Przywracanie całych systemów operacyjnych, ● Przywracanie Exchange bezpośrednio do serwera. ● Przywracanie Hyper-V bezpośrednio do hosta maszyn, ● Przywracanie Exchange 2013 na poziomie pojedynczej skrzynki, ● Usuwanie plików przesłanych jako backup, ● Usuwanie wybranej wersji pliku, ● Wyszukiwanie plików w repozytorium użytkownika, ● Nadpisywanie plików podczas ich przywracania. **Synchronizacja** Automatyczne przesyłanie plików z wybranego katalogu na serwer backupu oraz pobieranie plików przesłanych przez inne urządzenia w ramach konta użytkownika. W jej skład wchodzą: ● Synchronizacja wybranego katalogu, ● Wstrzymywanie oraz wznawianie synchronizacji, ● Zmiana katalogu synchronizowanego, ● Lista synchronizowanych plików, ● Wyłączanie synchronizacji, ● Szyfrowanie synchronizowanych plików. **Magazyn** Dane backupów powinny być przechowywane w minimum 2 profesjonalnych, certyfikowanych DataCenter na terenie Polski, oddalonych od siebie o minimum 300km **Ustawienia** Użytkownik końcowy powinien móc konfigurować zainstalowaną aplikację w następującym zakresie: ● Zmiana języka aplikacji, ● Automatyczne logowanie, ● Zapamiętywanie danych logowania, ● Automatyczne uruchamianie programu przy starcie systemu, ● Eksport oraz import konfiguracji do pliku, ● Eksport oraz import konfiguracji na serwer,

		● Ograniczenie ilości przechowywanych wersji, ● Ustawianie priorytetu dla procesu backupu, ● Zmiana klucza szyfrującego, ● Ustawienia proxy, ● Ustawienia przepustowości/zajętości pasma, ● Konfiguracja wydajności procesu backupu, ● Możliwość ograniczenia obciążenia dysku twardego, ● Możliwość wyłączenia zdalnego zarządzania. Aktualizacje Aplikacja kliencka może być aktualizowana na 2 sposoby: ● Automatycznie, ● Ręcznie **Bezpieczeństwo** Za bezpieczeństwo plików przesyłanych za pomocą aplikacji powinny odpowiadać następujące funkcje: ● Zastąpienie nazwy pliku GUID-em, ● Szyfrowanie danych algorytmem AES 256 CBC zawsze po stronie komputera użytkownika, ● Kompresja danych, ● Transmisja po bezpiecznym protokole SSL, ● Deklaracja domyślnego klucza szyfrującego, ● Deklaracja klucza szyfrującego użytkownika, ● Zmiana klucza szyfrującego, ● Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, ● Obliczanie sumy kontrolnej SHA-1, Aplikacja powinna obsługiwać co najmniej dwa języki: ● polski ● angielski **OPCJONALNA APLIKACJA CLI** Aplikacja CLI jest aplikacją JAVA obsługiwaną z linii komend. Posiada ona silnik backupu spójny z silnikiem backupu aplikacji Windows przez co proces backupu realizowany jest w jednakowy sposób. ● Jedynie backup plikowy ● Wbudowana pomoc **CENTRALNE ZARZĄDZANIE** ● Zdalne zarządzanie aplikacjami klienckimi,

		● Tworzenie i edycja użytkowników, ● Zdalne tworzenie zadań backupu, ● Wyzwalanie backupów na aplikacjach klienckich, ● Edycja projektów backupów zapisanych na urządzeniach końcowych, ● Przywracanie danych, które zostały poddane backupowi, na urządzenie użytkownika, ● Zdalna konfiguracja utylizacji zasobów komputera klienckiego przez aplikacje podczas wykonywania backupu, ● Wgląd do dziennika zdarzeń poszczególnych użytkowników platformy, ● Grupowanie projektów w szablony, ● Zarządzanie szablonami backupów, ● Przesyłanie zdefiniowanych szablonów do aplikacji klienckich, ● Zarządzanie sesjami backupu, ● Zdalna i cicha instalacja, ● Pobieranie informacji na temat urządzeń użytkowników aplikacji klienckich, ● Pobieranie aplikacji klienckich, ● Możliwość raportowania błędów, ● Generowanie raportów oraz wykresów, ● Zarządzanie szablonami backupu, ● Monitorowanie sesji, ● Dodawanie nowych oraz edycja istniejących klientów, ● Przegląd stanu licencji, ● Wykresy oraz statystyki, ● Wskazywanie statusu połączenia z serwerem, **APLIKACJE MOBILNE** Aplikacja powinna mieć możliwość zainstalowania na Android oraz iOS **PANEL WEB DLA UŻYTKOWNIKA** ● Zarządzanie użytkownikami w ramach licencji, ● Ustawianie klucza szyfrującego, ● Reset klucza szyfrującego, ● Usuwanie hostów, ● Wyświetlanie oraz pobieranie plików przesłanych jako backup, ● Bezpieczna transmisja za pośrednictwem protokołu SSL, ● Tworzenie linków publicznych dla plików znajdujących się w Aktówce, ● Możliwość definiowania ważności linku, ● Możliwość zmiany ważności linku, ● Możliwość wysłania linku mailem bezpośrednio z panelu, ● Możliwość zarządzania linkami, ● Możliwość wyboru użytkowników do współdzielenia z listy,

		● Możliwość zarządzania zasobami współdzielonymi, ● Możliwość wysłania zaproszenia do systemu, ● Dostęp do dziennika zdarzeń, ● Konfiguracja powiadomień mailowych, ● Zmiana oraz reset hasła użytkownika, ● Rozróżnianie typu urządzeń z którego pochodzi backup, ● Zarządzanie licencją– Modyfikacja, przedłużenie. ● Zarządzanie podziałem przestrzeni pomiędzy użytkownikami. **ARCHITEKTURA SYSTEMU** ● Architektura Klient- - Serwer, ● Aplikacje klienckie wyposażone w mechanizm wydajnego cache, ● Możliwość pełnej redundancji elementów systemu, **WSPIERANE SYSTEMY OPERACYJNE** ● Microsoft Windows 7 i nowsze ● Microsoft Windows Server 2008 R2 i nowsze ● Unix/Linux, ● OS X, ● Novell NetWare 6.5. ● Android ● iOS Licencjonowanie ● Licencja subskrypcyjna, obowiązująca przez okres minimum 12 miesięcy, ● Licencjonowanie nie ogranicza ilości zabezpieczanych stacji - jedynym limitem jest zajętość magazynu ● Magazyn chmurowy powinien mieć pojemność minimum 300 GB

2) Migracja oprogramowania antywirusowego

Zakup licencji na oprogramowanie antywirusowe – migracja do wyższej wersji
Migracja oprogramowania antywirusowego do wersji Eset Protect Entry ON-PREM dla 28 stanowisk.

3) Oprogramowanie do zarządzania infrastrukturą

Zakup oprogramowania do zintegrowanego zarządzania IT + jego instalacja Szczegółowy opis: Oprogramowanie do monitorowania i inwentaryzowania zasobów systemu informatycznego dla 28 stanowisk.

1	Oprogramowanie do inwentaryzacji systemu informatycznego.	Oprogramowanie powinno posiadać budowę modułową składającą się z serwera zarządzającego, konsoli i agentów Komunikacja pomiędzy Serwerem a Agentami i Konsolami musi być nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2.

		Oprogramowanie powinno być zbudowane z modułów i licencjonowane co najmniej dla modułów umożliwiających inwentaryzowanie zasobów sieciowych, inwentaryzację sprzętu, monitoring użytkowników i ochronę danych. Aplikacja powinna wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source. Instalacja Serwera oraz Konsol zarządzających powinna umożliwiać instalację na 64-bitowych systemach operacyjnych Windows. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, powinien być objęty kontrolą na poziomie wybranych Administratorów. Aplikacja musi umożliwiaj nadawanie kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Aplikacja powinna logować działania administratorów aplikacji oraz umożliwiać ich eksport do serwera logów.
2	Moduł sieciowy	Moduł sieciowy powinien pozwolić na wykrywanie w sieci urządzeń takich serwery fizyczne lub wirtualne pod kontrolą takich systemów jak Windows, Linux, Unix, Mac, wykrywanie routerów, przełączników, punktów dostępowych oraz telefonów VoIP oraz urządzeń mobilnych. Moduł powinien móc skanować sieć, integrować się z Active Directory, wizualizować mapę sieci komputerowej wraz z tworzeniem grup. Moduł powinien móc monitorować serwery pocztowe oraz serwery www oraz powinien móc obsługiwać szyfrowanie SSL/TLS oraz zapewnić obsługę komunikatów SNMP Aplikacja powinna mieć możliwość integracji z bramką SMS.
3	Moduł inwentaryzacji	Moduł inwentaryzacji powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu stacji roboczych oraz przedstawiać informacje o modelu sprzętu, procesora, pamięci itp. Aplikacja powinna móc przygotować zestawienie konfiguracji sprzętowych, wykorzystania zasobów systemu operacyjnego, informacji o zainstalowanych aplikacjach wraz z zestawieniem kluczy licencyjnych oraz zestawienie przechowywanych plików według rozszerzenia. Moduł powinien posiadać możliwość prowadzenia bazy ewidencji majątku w zakresie sprzętu i oprogramowania, generowania kodów kreskowych oraz kodów QR dla zasobów, generowania protokołów przekazania, możliwości inwentaryzowania za pomocą aplikacji na system Android.

4	Moduł do obsługi użytkowników	Moduł powinien móc monitorować aktywność użytkowników pracujących na komputerach. W skład monitorowanych aktywności powinny wchodzić: czas aktywności, czas uruchamianych procesów, czas rzeczywistego użytkowania programów, informacje o używanych dokumentach, listy odwiedzanych stron www, informacje o wydrukach, informacje o nagłówkach poczty elektronicznej. Dodatkowo wymagana jest możliwość blokowania: stron internetowych, blokowanie pobierania plików, wysyłania powiadomień o niechcianych działaniach użytkownika.
5	Moduł ochrony danych	Moduł musi mieć następujące funkcje: blokowanie urządzeń i nośników danych takich jak USB, FireWire, karty pamięci, dyski przenośnie, SATA, klawiatura, mysz, napędy optyczne i stacje dyskietek. Blokowanie sieci bezprzewodowych oraz Bluetooth, Aplikacja musi alarmować o zdarzeniach związanych z podłączaniem , odłączaniem urządzeń zewnętrznych. Aplikacja musi się integrować z Windows Defender oraz BitLocker oraz monitorować TPM. Moduł musi się integrować z Active Directory w celu definiowania reguł w połączeniu z grupami.
6	Licencjonowanie	Licencja wieczysta dla 28 urządzeń, 12 miesięcy umowy serwisowej na aktualizacje i pomoc techniczną. Możliwość zwiększenia liczby zarządzanych stacji roboczych w dowolnym czasie.
7	Wdrożenie i dostawa	Instalacja na wskazanym przez administratora systemie wraz z podstawowym uruchomieniem oraz instalacja agentów na komputerach klienckich.

4) Zakup oprogramowania

Szczegółowy opis: Zakup i dostawa nowych, legalnych pięciu licencji przeznaczonych na polski rynek pakietów biurowych Microsoft Office. Szczegółowy opis:

a) Licencja w postaci klucza produktu umieszczona w oryginalnym zafoliowanym pudełku,
b) Typ licencji: komercja/biznesowa, wieczysta
c) Język: polska wersja językowa
d) Wersja pakiety: najnowsza dostępna na polskim rynku
e) System operacyjny: Windows lub więcej
f) Zawartość pakietu: edytor teksu Word, arkusz kalkulacyjny Excel, edytor prezentacji multimedialnych PowerPoint, klient poczty elektronicznej Outlook, system notatek elektronicznych OneNote
g) Zamawiający dopuszcza rozwiązania równoważne. Za rozwiązanie równoważne uznane zostaną pakiety biurowe posiadające w 100% tożsame funkcjonalności i obsługę formatów plików określone na stronie internetowej producenta oraz właściwości określone w podpunktach a-f.

W związku z tym, że pracownicy Zamawiającego są przeszkoleni z obsługi pakietu biurowego Microsoft Office, w przypadku zaoferowania rozwiązania równoważnego Wykonawca będzie zobowiązany do przeszkolenia użytkowników proponowanego oprogramowania w poziomie średniozaawansowanym.