DOLNOŚLASKIE CENTRUM LECZENIA UZALEŻNIEŃ
W CZARNYM BORZE
58-379 Czarny Bór, ul. Parkowa 8
tel. (74) 84 50 125, fax (74) 84 50 290, e-mail: sekretariat@dclu.pl www.dclu.pl

Czarny Bór, 18-10-2023

Numer sprawy: DCLU/ZP/3/2023

Do:

Wszyscy Wykonawcy

Zmiana treści SWZ

Dotyczy postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji na: **Dostawa infrastruktury ICT i oprogramowania na potrzeby projektu cyberbezpieczeństwo dla Dolnośląskiego Centrum Leczenia Uzależnień w Czarnym Borze**.

Działając na podstawie art. 286 ust. 1 ustawy z dnia 11 września 2019r. - Prawo zamówień publicznych Zamawiający dokonuje zmiany treści SWZ:

Zamawiający zmienia zapis załącznika nr 1 do SWZ Szczegółowy opis przedmiotu zamówienia, który otrzymuje następujące brzmienie:

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Urządzenia i oprogramowanie zabezpieczające sieć (UTM/firewall) – 2 sztuki**
   Dostawa urządzeń wraz z wdrożeniem, wsparciem technicznym i aktualizacjami

Specyfikacja:

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, usług internetowych (web services), 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).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

13. 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.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. 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.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.

19. 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.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. 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).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
23. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci.
24. Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

25. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
26. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
27. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
28. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

29. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
30. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
31. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
32. 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.
33. Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym.

OCHRONA ANTYSPAM

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

WIRTUALNE SIECI PRYWATNE (VPN)

38. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
39. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
40. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
41. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
42. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
43. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
44. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
45. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

46. Urządzenie ma posiadać wbudowany filtr URL.
47. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych.

48. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
49. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
50. Administrator ma mieć możliwość dodawania własnych kategorii URL.
51. 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.
52. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
53. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
54. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
55. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
56. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
57. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

58. 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.
59. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
60. 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.
61. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

62. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
63. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
64. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
65. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
66. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

67. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
68. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia.
69. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
70. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
71. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
72. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
73. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

74. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
75. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
76. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

77. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

78. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
79. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
80. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
81. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
82. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
83. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
84. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
85. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
86. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
87. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
88. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
89. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
90. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
91. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
92. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
93. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
94. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
95. 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 serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

96. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

97. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

98. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

99. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

100. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

101. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.

102. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.

103. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.

104. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.

105. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.

106. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.

107. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

108. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

109. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

110. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).

111. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

112. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
113. Urządzenie ma posiadać usługę DNS Proxy.
114. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
115. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
116. Urządzenie musi mieć zaimplementowane Open API
117. 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

118. Urządzenia mają być objęte 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
119. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

120. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.
121. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.
122. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16.
123. Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10.
124. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:
    a. Moduł z 8 interfejsami miedzianymi 2,5Gbps
    b. Moduł z 4 interfejsami miedzianymi 10Gbps.
    c. Moduł z 4 interfejsami światłowodowymi 1Gbps.
    d. Moduł z 8 interfejsami światłowodowymi 1Gbps.
    e. Moduł z 4 interfejsami światłowodowymi 10Gbps.
125. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
126. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.

127. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps.
128. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps.
129. Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps.
130. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps.
131. Maksymalna liczba tuneli VPN IPSec – minimum 1000.
132. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.
133. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 150.
134. Obsługa interfejsów 802.11q (VLAN) – minimum 256.
135. Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę.
136. Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive.
137. Urządzenie nie ma limitu na liczbę użytkowników.
138. Liczba reguł filtrowania – minimum 16 384.
139. Liczba tras statycznego routingu – minimum 5 120.
140. Liczba tras dynamicznego routingu – minimum 10 000.
141. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.
142. Urządzenie musi być wyposażone w moduł TPM.

2. Urządzenia i oprogramowanie zabezpieczające sieć (UTM/firewall) – 4 sztuki

Dostawa urządzeń wraz z wdrożeniem, wsparciem technicznym i aktualizacjami

Specyfikacja:

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, usług internetowych (web services), 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).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

13. 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.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. 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.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. 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.

20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. 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).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

27. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
28. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
29. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
30. 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

31. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
32. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.

33. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
34. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

35. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
36. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
37. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
38. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
39. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
40. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
41. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
42. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

43. Urządzenie ma posiadać wbudowany filtr URL.
44. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
45. Administrator ma mieć możliwość dodawania własnych kategorii URL.
46. 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.

47. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
48. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
49. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
50. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
51. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
52. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

53. 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.
54. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
55. 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.
56. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
57. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
58. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
59. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
60. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
61. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

62. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
63. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia.
64. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
65. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
66. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
67. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
68. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

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

ADMINISTRACJA URZĄDZENIEM

73. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
74. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
75. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
76. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

77. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
78. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
79. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
80. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
81. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
83. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
84. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
85. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
86. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
87. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
88. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
89. 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 serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
90. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
91. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
92. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

93. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

94. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
95. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
96. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
97. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
98. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
99. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
100. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
101. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

102. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
103. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
104. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
105. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
106. Urządzenie ma posiadać usługę DNS Proxy.
107. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
108. Urządzenie musi mieć zaimplementowane Open API
109. 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.
110. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
111. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

GWARANCJA I SERWIS

112. Urządzenie ma być objęte 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
113. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

114. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
115. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
116. Liczba portów Ethernet 2,5Gbps – min. 8.
117. Liczba portów światłowodowych 1Gbps – min. 1.
118. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
119. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
120. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
121. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
122. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
123. Maksymalna liczba tuneli VPN IPSec – minimum 100.
124. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
125. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
126. Obsługa interfejsów 802.11q (VLAN) – minimum 128
127. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
128. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
129. Urządzenie nie ma limitu na liczbę użytkowników.
130. Liczba reguł filtrowania – minimum 8 192.
131. Liczba tras statycznego routingu – minimum 512.
132. Liczba tras dynamicznego routingu – minimum 10 000.
133. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.

134. Urządzenie musi być wyposażone w moduł TPM.

3. System do tworzenia kopii danych – 1 sztuka

Dostawa urządzenia wraz z wdrożeniem, wsparciem technicznym i aktualizacjami

Specyfikacja:

Ogólne:

- System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.
- Konsola zarządzająca może być również instalowana w chmurze producenta zlokalizowanej na terenie Polski,
- Interfejs systemu dostępny jest w języku:
    - polskim,
    - angielskim,
    - ukraińskim,
- System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji, w tym z możliwością odtworzenia w postaci usługi uruchomionej w chmurze producenta zlokalizowanej na terenie Polski,
- Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej),
- Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.

Sprzętowe:

· Obudowa: Rack 1u,

· Procesor: min. 6 rdzeni, min. 12 wątków, taktowanie min. 2.9GHz

· Pamięć RAM: min. 16 GB DDR4

· Przestrzeń dostępna przy konfiguracji RAID 5 : min. 24 TB

· Osobne dyski NVME 2x 240GB na konsolę zarządzającą

· Urządzenie powinno posiadać już zainstalowane dyski oraz skonfigurowany RAID 5 i być gotowe do pracy zgodnie z pkt. 1 opisu przedmiotu zamówienia,

- Redundantne zasilanie 2x 600 W
- Interfejsy sieciowe: 2szt. 1Gb Ethernet
- Gwarancja NBD on-premise na min. 3/5 lat

Wsparcie techniczne:

- Pomoc techniczna w językach:
  - polskim,
  - angielskim.
- Świadczone jest bezpośrednio przez główną siedzibę producenta.
- Materiały samopomocowe
  - Baza wiedzy,
  - Nagrania wideo,
  - Karty produktowe

Zarządzanie:

- Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli, dostępnej za pośrednictwem przeglądarki WWW,
- Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,
- Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,
- Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,
- Monitorowanie postępu działania zadania,
- Posiada system powiadamiania poprzez e-mail bądź Slack o zdarzeniach w następujących przypadkach:
  - Zadanie zostało zakończone pomyślnie,
  - Zadanie zostało zakończone z ostrzeżeniami,

- Zadanie zostało zakończone z błędem,
- Zadanie zostało anulowane,
- Zadanie nie zostało uruchomione.

- System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego
- System umożliwia wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
- Możliwość zdefiniowania okna backupowego dla każdego z zadań,
- Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów i innych sekretów, wykorzystywanych przez System,
- System pozwala na klonowanie planów kopii zapasowych,
- System umożliwia reset hasła administratora w przypadku jego utraty,
- Oprogramowanie umożliwia definiowanie retencji według schematów:
  - GFS(Grandfather-Father-Son),
  - FIFO(First-In, First-Out).
- Oprogramowanie umożliwia tworzenie grup urządzeń,
- Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
- System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:
  - System Administrator,
  - Backup operator,
  - Restore operator,
  - Viewer.
- Administrator Systemu powinien mieć możliwość logowania się z wykorzystaniem kont Google,

Składowanie danych:

- Dane są składowane w ramach dostępnej macierzy wymienionej w wymaganiach sprzętowych OPZ
- Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach:
    - Lokalnie:
        - Zasób SMB,
        - Zasób NFS,
        - Zasób ISCSI,
        - Zasób S3,
        - Katalog zabezpieczonego urządzenia.
    - W chmurze:
        - Amazon Web Service,
        - Magazyn zgodny z S3,
        - Dostarczanej przez producenta.
- System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
- System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
- System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych,
- System obsługuje mechanizm WORM (Write Once Ready Many) w chmurowych oraz lokalnych repozytoriów kopii,
- System umożliwia replikację danych na własne zasoby.

Odtwarzanie:

- Odtwarzanie granularne:
    - Pojedynczych plików z kopii obrazu dysku,

- Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.

- Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
  - Windows: 7+,
  - Windows Server: 2008 R2+,
- Odtwarzanie Bare Metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
- Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a,
- Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.
- Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(RAW, VHD, VHDX, VMDK),
- Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),
- Odtwarzanie zasobów plikowych z prawami dostępu,
- Przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows),
- Odtwarzanie danych według harmonogramu,
- Przywracanie danych z określonego urządzenia/użytkownika,
- Przywracanie kopii z wybranego magazynu.
- Przywracanie danych Microsoft 365:
  - do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst
  - do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),
- System posiada możliwość nieodwracalnego kasowania danych,
- Przywracanie repozytoriów GIT:
  - Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket/GitLab),
  - przywracanie między kontami.

Backup:

- Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych dla:
  - Systemów operacyjnych:
    - Alpine 3.10+,
    - Debian: 9+,
    - Ubuntu: 16.04+,
    - Fedora: 29+,
    - centOS: 7+,
    - RHEL: 6+,
    - openSUSE: 15+,
    - SUSE Enterprise Linux(SLES): 12 SP2+,
    - macOS: 10.13+,
    - Windows: 7 i nowsze
    - Windows Server: 2008 R2 i nowsze
  - Środowisk wirtualnych:
    - Hyper-V,
    - VMware,
    - Dowolnych innych – agentowo.
  - Repozytoriów GIT:
    - GitHub,
    - Bitbucket
    - GitLab
  - Jira Cloud
- Wykonywanie pełnych, różnicowych oraz przyrostowych kopii zapasowych dla:
  - Baz danych**:**

- Microsoft SQL,
- MySQL,
- PostgreSQL,
- Firebird,
- Oracle
- Dowolnych innych przez podpięcie skryptów pre/post.

- Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:
  - 128 bit,
  - 192 bit,
  - 256 bit.
- Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:
  - ZStandard,
  - LZ4.
- Oprogramowanie umożliwia zarządzanie poziomem kompresji,
- System dostarcza agenta backupu w postaci kontenera Docker, umożliwiajacego wykonywanie kopii zapasowych z dowolnych środowisk kontenerowych, w tym popularnych rozwiązań NAS,
- System dostarcza agenta backupu w postaci instalatora MSI, umożliwiającego masową instalację w systemach Windows z wykorzystaniem narzędzi Active Directory - SCCM oraz GPO
- Wykonywanie kopii zapasowej otwartych plików(VSS),
- System umożliwia uruchamianie skryptów przed i po backupie,
- System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,
- System umożliwia wykonywanie spójnej kopii danych pracujących aplikacji na urządzeniach z systemem Windows oraz wspieranych środowiskach wirtualnych,
- System pobiera jedynie zmodyfikowane bloki danych podczas przyrostowej i różnicowej kopii maszyn wirtualnych VMware,
- System umożliwia wykonywanie kopii maszyn wirtualnych VMware z zastosowanie zaawansowanych trybów transportu (HotAdd, LAN, SAN), w tym metodą LAN-Free,

- System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,
- Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,
- Backup plikowy,
- Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,
- Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,
- Oprogramowanie pozwala na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej,
- Oprogramowanie pozwala na backup zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption

GIT

- Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych),
- Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).

Licencjonowanie:

- Licencje powinny pozwalać na:
    - Zabezpieczenie nielimitowanej ilości maszyn wirtualnych
    - Zabezpieczenie nielimitowanej ilości serwerów fizycznych
    - Zabezpieczenie nielimitowanej ilości stacji roboczych
    - Przechowywanie danych w chmurze dostarczonej bezpośrednio przez producenta systemu z przestrzenią 4.8 TB na okres 3/5 lat.
    - Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu
- Wsparcie techniczne:
    - Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta,
    - Zapewnia dostęp do aktualizacji oprogramowania,

- Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,
- Obowiązuje przez okres minimum 36 miesięcy.

Zamawiający zmienia zapis Rozdziału XIX SWZ, który otrzymuje następujące brzmienie:

XIX. **Termin związania ofertą.**

1. Termin związania ofertą wynosi **30 dni** od upływu terminu składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą wskazanego w pkt. 1 zamawiający przed upływem terminu związania ofertą zwraca jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany prze niego okres, nie dłuższy niż 30 dni. Przedłużenie terminu związania ofertą wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
3. Termin związania ofertą upływa: **22-11-2023r.**

Zamawiający zmienia zapis Rozdziału XXI SWZ, który otrzymuje następujące brzmienie:

XXI. **Miejsce oraz termin składania ofert.**

1. Ofertę oraz oświadczenie, o którym mowa w art. 125 ust. 1 Pzp, składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
2. Oferty, oświadczenia, o których mowa w art. 125 ust. 1 Pzp, oświadczenie, o którym mowa w art. 117 ust. 4 Pzp, zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w art. 118 ust. 3 Pzp oraz pełnomocnictwo, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne z zastrzeżeniem formatów, o których mowa w art. 66 ust. 1 Pzp, z uwzględnieniem rodzaju przekazywanych danych.

A. **Sposób składania ofert.**

Miejsce i termin składania ofert

Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem : https://platformazakupowa.pl/transakcja/828718 w myśl Ustawy na stronie internetowej prowadzonego postępowania do dnia

24-10-2023r. godz. 09:00

Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.

Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania”.

Oferta lub wniosek składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem platformazakupowa.pl, wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust 1 oraz ust.2 Pzp, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust.1 sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku “Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.

Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

DOLNOŚLASKIE CENTRUM LECZENIA UZALEŻNIEŃ
W CZARNYM BORZE
58-379 Czarny Bór, ul. Parkowa 8
tel. (74) 84 50 125, fax (74) 84 50 290, e-mail: sekretariat@dclu.pl www.dclu.pl

Zamawiający zmienia zapis Rozdziału XXII SWZ, który otrzymuje następujące brzmienie:

XXII. **Termin otwarcia ofert.**

1. Otwarcie ofert następuje niezwłocznie po upływie terminu składania ofert tj. **24-10-2023 r. godz. 09:15**, (nie później niż następnego dnia po dniu, w którym upłynął termin składania ofert).

2. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.

3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

4. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

5. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:

1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;

2) cenach lub kosztach zawartych w ofertach.

Informacja zostanie opublikowana na stronie postępowania na platformazakupowa.pl w sekcji ,,Komunikaty” .

Zgodnie z Ustawą Prawo Zamówień Publicznych Zamawiający nie ma obowiązku przeprowadzania jawnej sesji otwarcia ofert w sposób jawny z udziałem wykonawców lub transmitowania sesji otwarcia za pośrednictwem elektronicznych narzędzi do przekazu wideo on-line a ma jedynie takie uprawnienie.

DOLNOŚLASKIE CENTRUM LECZENIA UZALEŻNIEŃ
W CZARNYM BORZE
58-379 Czarny Bór, ul. Parkowa 8
tel. (74) 84 50 125, fax (74) 84 50 290, e-mail: sekretariat@dclu.pl www.dclu.pl

Zamawiający zmienia zapis załącznika nr 4 do SWZ Wzór umowy, który otrzymuje następujące brzmienie:

UMOWA nr ……..

zawarta w dniu …… r.

1./ **DOLNOŚLĄSKIM CENTRUM LECZENIA UZALEŻNIEŃ W CZARNYM BORZE,** adres: ul. Parkowa 8, 58-379 Czarny Bór, dla którego Sąd Rejonowy dla Wrocławia-Fabrycznej we Wrocławiu, XI Wydział Gospodarczy Krajowego Rejestru Sądowego prowadzi dokumentację zakładu, wpisanym do Rejestru Stowarzyszeń, Innych Organizacji Społecznych I Zawodowych, Fundacji Oraz Samodzielnych Publicznych Zakładów Opieki Zdrowotnej Krajowego Rejestru Sądowego pod numerem KRS 0000085329, NIP 8862385284,
reprezentowanym przez Dyrektora Marka Zawadę
zwanym dalej w tekście **„Zamawiającym”**,

a

2./……
reprezentowaną przez:
…….

zwaną dalej **„Wykonawcą”**,

zwanymi dalej również **"Stronami".**

Umowa zostaje zawarta na podstawie ustawy z dnia 11.09.2019 r. Prawo zamówień publicznych, po przeprowadzeniu zamówienia publicznego pn. „*Dostawa infrastruktury ICT oraz oprogramowania na potrzeby projektu cyberbezpieczeństwo dla Dolnośląskiego Centrum Leczenia Uzależnień w Czarnym Borze”,* znak DCLU/ZP/3/2023*.*

§ 1
Przedmiot Umowy

1. Przedmiotem Umowy jest *dostawa* ***oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych wraz z wykonaniem usług podnoszących***

bezpieczeństwo systemów IT w ramach środków pochodzących z Funduszu Przeciwdziałania COVID-19 - podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców dla potrzeb Dolnośląskiego Centrum Leczenia Uzależnień w Czarnym Borze, w tym:

1) Urządzenia i oprogramowanie zabezpieczające sieć (UTM/firewall) w klastrze wysokiej dostępności – dostawa wraz z wdrożeniem, wsparciem technicznym i aktualizacjami – 2 sztuki
2) Urządzenia i oprogramowanie zabezpieczające sieć (UTM/firewall) – dostawa urządzeń wraz z wdrożeniem, wsparciem technicznym i aktualizacjami – 4 sztuki
3) System do tworzenia kopii danych – dostawa urządzenia wraz z wdrożeniem, wsparciem technicznym i aktualizacjami – 1 sztuka

2. Szczegółowy opis dostaw i usług zawiera Opis Przedmiotu Zamówienia stanowiący Załącznik nr 1 do Umowy.

§2
Oświadczenia i zapewnienia Stron

1. Wykonawca oświadcza, że posiada prawo świadczenia usług objętych Umową oraz że jest uprawniony do wprowadzania oprogramowania do obrotu i używania na terenie Polski, oraz że uprawnienie to nie wygasło, ani nie zostało odwołane, zbyte ani ograniczone.
2. Wykonawca oświadcza, że objęte niniejszą Umową oprogramowanie i sprzęt pochodzić będzie z oficjalnych kanałów dystrybucyjnych producenta obejmujących również rynek Unii Europejskiej, zapewniających w szczególności realizację uprawnień gwarancyjnych.
3. Wykonawca dostarczy sprzęt, który jest fabrycznie nowy, nieużywany, wolny od wad fizycznych i prawnych i nie jest przedmiotem praw lub roszczeń osób trzecich.
4. Wraz ze sprzętem, Wykonawca dostarczy wszelkie dokumenty dotyczące sprzętu, w szczególności dokumenty niezbędne do jego prawidłowej eksploatacji, sporządzone w języku polskim, w tym w szczególności instrukcję obsługi sprzętu oraz dokumenty gwarancyjne sprzętu potwierdzające fakt uzyskania przez Zamawiającego Głównego uprawnień gwarancyjnych (o ile dotyczy).
5. Strony deklarują współpracę w celu realizacji przedmiotu Umowy. W szczególności Strony zobowiązane są do wzajemnego powiadamiania się o ważnych okolicznościach mających lub mogących mieć wpływ na wykonanie przedmiotu Umowy, w tym na ewentualne opóźnienia.
6. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury oraz pomieszczeń niezbędnych do realizacji Umowy.

7. Zamawiający oświadcza, że jest świadomy konsekwencji braku dokonywania i weryfikacji poprawności kopii bezpieczeństwa danych i systemów, jak również nienależytego zabezpieczenia nośników i infrastruktury. Zamawiający zobowiązuje się do wykonania kopii bezpieczeństwa i weryfikacji jej poprawności przed przystąpieniem przez Wykonawcę do realizacji prac.
8. Wykonawca nie ponosi odpowiedzialności za szkody wywołane którąkolwiek z następujących okoliczności, a w wypadku ich wystąpienia Zamawiający nie będzie z tego tytułu wysuwał żadnych roszczeń do Wykonawcy:
   1) utrata danych,
   2) brak możliwości odtworzenia utraconych danych,
   3) utrudnienie w korzystaniu lub całkowita utrata możliwości eksploatacji, Oprogramowania Aplikacyjnego lub innych programów, jeżeli jest spowodowana utratą danych,
   4) zaniechanie Zamawiającego, w należytym zabezpieczaniu Infrastruktury
   5) zmasowany atak zewnętrzny tzw. DoS,
   6) zaniechanie Zamawiającego, w należytym zabezpieczaniu danych identyfikacyjnych umożliwiających dostęp do HD osobom trzecim,
   7) wszystkie szkody będące następstwami okoliczności wymienionych powyżej lub wynikające z powodu okoliczności za które wyłącznej odpowiedzialności nie ponosi Wykonawca.

§ 3
Osoby upoważnione do kontaktu

1. Osobą upoważnioną do kontaktów oraz odbioru przedmiotu Umowy ze Strony Zamawiającego jest:
   imię, nazwisko: **……..**
   numer telefonu: **……., *email:* …….**
2. Osobą upoważnioną ze strony Wykonawcy jest:
   imię, nazwisko: **…….**
   numer telefonu: **……., *email:* …….**
3. Strona poinformuje drugą stronę niniejszej Umowy, na piśmie pod rygorem nieważności, o każdorazowej zmianie osoby uprawnionej do kontaktów, zmianie jej danych, a w szczególności zmianie numerów telefonów.

§4
Zasady dostawy i wdrożenia

1. Dostawa i wdrożenie przedmiotu Umowy nastąpi na koszt i ryzyko Wykonawcy. Dostawa nastąpi dowolnym środkiem transportu do siedziby Zamawiającego – Miejsca Dostawy tj. ul. Parkowa 8, 58-379 Czarny Bór.
2. Wykonawca dostarczy przedmiot Umowy do Miejsca Dostawy i rozmieści/zainstaluje je w miejscach wskazanych przez Zamawiającego.
3. Wykonawca oświadcza, że zapoznał się z warunkami i możliwościami dostawy oraz rozmieszczenia lub instalacji przedmiotu Umowy w Miejscu Dostawy.
4. Wykonawca oświadcza, że przedmiot Umowy jest sprawny oraz kompletny i po jego dostawie oraz rozmieszczeniu/zainstalowaniu/uruchomieniu Zamawiający bez żadnych dodatkowych kosztów będzie mógł przystąpić do jego używania.
5. Strony akceptują fakt, że usługi wdrożeniowe, szkoleniowe i serwisowe mogą być wykonywane poza siedzibą Zamawiającego lub zdalnie.
6. Zamawiający zapewni Wykonawcy możliwość instalacji urządzeń lub oprogramowania narzędziowego, umożliwiających zdalny, bezpieczny szyfrowany dostęp do infrastruktury, w szczególności serwera/ów, na którym/ch posadowione jest serwisowane oprogramowanie, środowisko systemowe oraz MBD wraz z bazą danych.

§ 5
Termin i odbiór przedmiotu Umowy

1. Wykonawca zobowiązany jest do wdrożenia prawidłowo zamówionego przedmiotu Umowy w terminie do **14 dni** od podpisania umowy. Zamawiający dopuszcza realizację i odbiory Umowy w podziale na etapy, uzgodnione przez Strony.
2. Odbiór końcowy przedmiotu niniejszej Umowy będzie potwierdzony protokołem bezusterkowego odbioru końcowego podpisanym przez Zamawiającego i Wykonawcę.
3. O gotowości do odbioru przedmiotu Umowy Wykonawca powiadamiać będzie Zamawiającego, który w terminie 3 dni od powiadomienia o gotowości do odbioru przedmiotu Umowy jest zobligowany do podpisania protokołu odbioru ewentualnie wyspecyfikuje w tym terminie swoje zastrzeżenia co do niezgodności przedmiotu odbioru z przedmiotem Umowy.
4. Jeżeli bez uzasadnionej przyczyny Zamawiający nie przystąpi w przewidzianym Umową terminie do procedury odbioru lub bez uzasadnionej przyczyny odmówi podpisania jakiegokolwiek protokołu, Wykonawcy przysługuje prawo dokonania odbioru jednostronnego oraz jednostronnego sporządzenia i podpisania protokołu, z zaznaczeniem przyczyny odmowy złożenia podpisu przez

Zamawiającego, co wywołuje skutki identyczne z podpisaniem protokołu przez obydwie Strony.

5. W przypadku stwierdzenia przez Zamawiającego wad/ uszkodzeń/ zastrzeżeń / braków ilościowych podczas odbioru etapu/usług lub całego przedmiotu niniejszej Umowy Zamawiający sporządzi protokół stwierdzający nieprawidłowości i/lub braki, a Wykonawca zobowiązuje się wymienić przedmiot zamówienia na pełnowartościowy lub uzupełnić braki, w terminie do 7 dni lub innym, uzgodnionym przez Strony w protokole i ponownie zgłosi gotowość do odbioru.
6. Dostawa przedmiotu Umowy do Miejsca Dostawy opisanego w SWZ oraz montaż/ instalacja/rozmieszczenie/uruchomienie nastąpi w terminie uzgodnionym z Zamawiającym.
7. Za termin wykonania Umowy rozumie się datę zgłoszenia gotowości do odbioru przedmiotu odbioru.

§ 6
Wynagrodzenie i warunki płatności

1. Wynagrodzenie za wykonanie wszystkich obowiązków Wykonawcy w ramach niniejszej Umowy wynosi: ……... zł netto (słownie: ……..) plus obowiązująca stawka podatku VAT, to jest łącznie …… zł brutto (słownie: …….).
2. Ustalone wynagrodzenie jest wynagrodzeniem ryczałtowym, zgodnie ze Specyfikacją Warunków Zamówienia oraz wybraną w trybie postępowania ofertą Wykonawcy, jest niezmienne przez okres realizacji Umowy i obejmuje wszystkie koszty Wykonawcy niezbędne do realizacji niniejszej Umowy zarówno w okresie dostaw, przeszkolenia jak i w okresie udzielonej gwarancji.
3. Wynagrodzenie zostanie wypłacone na podstawie faktury wystawionej po Odbiorze przedmiotu Umowy. Podstawą do wystawienia faktury jest protokół odbioru dostawy/usług bez uwag, o którym mowa w § 5 ust. 3 niniejszej Umowy.
4. Faktury będą płatne przelewem na rachunek bankowy wskazany przez Wykonawcę na fakturze w terminie 30 dni kalendarzowych od daty wystawienia prawidłowej faktury VAT,
5. Za datę zapłaty wynagrodzenia uważa się datę obciążenia rachunku bankowego Zamawiającego.
6. Za ewentualną nieterminową płatność Wykonawca może żądać zapłaty odsetek ustawowych.
7. Wykonawca oświadcza, że rachunek bankowy wskazany na fakturze jest tożsamy z rachunkiem bankowym wskazanym w rejestrze podatników podatku od towarów i usług, z zastrzeżeniem przypadku, gdy Wykonawca będzie zwolniony z podatku od towarów i usług. W przypadku, gdy rachunek wskazany na fakturze nie będzie zgodny z rachunkiem wskazanym w rejestrze podatku

od towarów i usług, a Wykonawca nie będzie podlegał zwolnieniu od podatku od towarów i usług, Zamawiający wzywa Wykonawcę do przedłożenia potwierdzenia zmiany rachunku bankowego w przedmiotowym rejestrze w terminie dwóch dni. Jeżeli Wykonawca nie przedstawi dokumentu potwierdzającego zmianę numeru rachunku bankowego w rejestrze podatników podatku od towarów i usług, Zamawiający ma prawo dokonania zapłaty wynagrodzenia na rachunek bankowy wskazany w rejestrze podatników podatku od towarów i usług. W tym wypadku, uznaje się, że Zamawiający prawidłowo wykonał swoje zobowiązanie w zakresie zapłaty wynagrodzenia, a Wykonawcy nie przysługują z tego tytułu żadne roszczenia.

8. Jeżeli Wykonawca nie posiada rachunku bankowego zarejestrowanego w rejestrze podatników podatku od towarów i usług oraz nie przedstawi dokumentu potwierdzającego braku obowiązku rejestracji tegoż rachunku bankowego, Zamawiający ma prawo do wstrzymania zapłaty wynagrodzenia do chwili potwierdzenia rejestracji rachunku bankowego przez Wykonawcę lub przedłożenia dokumentu potwierdzającego brak tegoż obowiązku. Strony zgodnie oświadczają, że wskazane okoliczności nie stanowią opóźnienia lub zwłoki Zamawiającego w zapłacie wynagrodzenia i nie mogą być podstawą jakichkolwiek roszczeń Wykonawcy wobec Zamawiającego.
9. Zamawiający dopuszcza możliwość złożenia faktury w postaci elektronicznej w rozumieniu art. 2 pkt 32 Ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług z uwzględnieniem art. 106e oraz 106g ww. Ustawy oraz art. 6 Ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym, obsługiwanych przez portal ……. Dostarczenie danych faktury w postaci elektronicznej zwalnia z dostarczenia faktury w postaci papierowej.

§ 7
Ochrona danych osobowych i zachowanie poufności

1. Każda ze stron Umowy oświadcza, iż jest Administratorem danych osobowych w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej RODO, w odniesieniu do danych osobowych swoich przedstawicieli oraz przedstawicieli drugiej Strony wskazanych w umowie jako osoby do kontaktu (tzw. dane kontaktowe) oraz osoby realizujące przedmiot Umowy. Przekazywane na potrzeby realizacji Umowy dane osobowe są danymi zwykłymi i obejmują w szczególności imię, nazwisko, zajmowane stanowisko i miejsce pracy, numer służbowego telefonu, służbowy adres email.

2. Dane osobowe osób, o których mowa w ust. 1, będą przetwarzane przez Strony na podstawie art. 6 ust. 1 lit. f) RODO (tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratorów danych) jedynie w celu i zakresie niezbędnym do wykonania zadań związanych z realizacją zawartej Umowy.
3. Strony zobowiązują się do ochrony danych osobowych udostępnionych wzajemnie w związku z wykonywaniem Umowy, w tym do wdrożenia oraz stosowania środków technicznych i organizacyjnych zapewniających odpowiedni stopień bezpieczeństwa danych osobowych zgodnie z przepisami prawa, a w szczególności z ustawą z dnia 10.05.2018 r. o ochronie danych osobowych oraz przepisami RODO.
4. Strony zobowiązują się poinformować osoby fizyczne niepodpisujące niniejszą Umowę, o których mowa w ust. 1, o treści niniejszego paragrafu.
5. Wykonawca zobowiązuje się do przestrzegania zasad obowiązujących w zakresie ochrony danych osobowych zgodnie z obowiązującymi przepisami prawa – w szczególności w przypadku wdrożenia oraz przeglądów sprzętu w okresie trwania gwarancji, który zawiera dane osobowe.
6. W przypadku powierzenia Wykonawcy przez Zamawiającego do przetwarzania danych osobowych, których Administratorem jest Zamawiający, Strony zobowiązują się do zawarcia Umowy powierzenia przetwarzania danych osobowych.
7. Każda ze Stron jest zobowiązana do zachowania całkowitej poufności wszelkich istotnych informacji odnoszących się do drugiej Strony, oznaczonych jako poufne lub w przypadku których okoliczności przekazania informacji wskazują na obowiązek zachowania takich informacji w poufności (informacje poufne) zgodnie z postanowieniami niniejszego ustępu:
    1) Informację poufną stanowią informacje uzyskane przez Stronę od drugiej Strony w związku z wykonywaniem czynności określonych w Umowie, których ujawnienie osobom trzecim może narazić Stronę przekazującą te informacje na szkodę, w szczególności informacje stanowiące tajemnicę handlową i tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji oraz wszystkie informacje uzyskane w związku z realizacją zadań określonych Umową, w szczególności:
        a) treść i zawartość Zgłoszeń Serwisowych,
        b) treść komunikatów publikowanych w aplikacji do zgłoszeń serwisowych,
        c) dane osobowe,
        d) dane dotyczące zabezpieczeń,
        e) dane finansowe Zamawiającego oraz jego kontrahentów.
    2) Strony zobowiązane są zapobiec ujawnianiu, czy rozpowszechnianiu informacji poufnych drugiej Strony, uzyskanych w toku realizacji Umowy.

Każda ze Stron zobowiąże wszystkie osoby związane z wykonywaniem Umowy do zachowania poufności informacji poufnych drugiej Strony.

3) Obowiązek zachowania informacji poufnych obowiązuje Strony przez okres wskazany w samych informacjach, towarzyszących im dokumentach lub mediach z wykorzystaniem których zostały przekazane lub jeżeli okres nie został wskazany, przez okres trzech lat po rozwiązaniu lub wygaśnięciu Umowy, bez względu na sposób i tryb rozwiązania lub wygaśnięcia. Zwolnienia Strony z obowiązku zachowania poufności dokonuje ta Strona, której dotyczą informacje poufne, na piśmie pod rygorem nieważności.
4) Obowiązku zachowania poufności nie stosuje się do informacji:
   a) powszechnie znanych w momencie ich ujawnienia;
   b) otrzymanych przez Stronę, zgodnie z powszechnie obowiązującymi przepisami prawa, od podmiotu uprawnionego bez obowiązku zachowania poufności;
   c) które w momencie ich przekazania były już znane Stronie bez obowiązku zachowania poufności;
   d) w stosunku do których Strona uzyskała pisemną zgodę drugiej Strony na ich ujawnienie (pod rygorem nieważności zgody na ujawnienie uzyskanej w innej niż pisemna formie).
5) Jeżeli ujawnienie informacji poufnej nastąpić ma na żądanie sądu lub innego upoważnionego organu władzy państwowej działającego zgodnie z prawem, Strona obowiązana do ujawnienia informacji poufnych zawiadomi o tym bezzwłocznie drugą Stronę, umożliwiając jej zajęcie stanowiska co do konieczności, zakresu lub formy takiego ujawnienia.
6) Jeżeli Strony nie postanowią inaczej na piśmie, wszelkie informacje poufne pozostaną własnością Strony, która ujawnia informacje poufne i zostaną jej zwrócone lub na jej pisemne żądanie zniszczone w dniu wygaśnięcia lub rozwiązania Umowy lub w innym terminie uzgodnionym przez upoważnionych przedstawicieli Stron.

§ 8
Gwarancja

1. Okres gwarancji na dostarczone urządzenia wynosi …… miesięcy (*zgodnie ze złożoną ofertą – minimum 36 miesięcy*), licząc od daty podpisania protokołu odbioru przedmiotu zamówienia. W okresie gwarancji Wykonawca zapewnia bezpłatne wykonywanie przeglądów serwisowych, a także tych czynności konserwacyjnych, które nie mogą być realizowane samodzielnie przez użytkownika.

2. W okresie gwarancji na dostarczone urządzenia Wykonawca zobowiązany jest bezpłatnie wykonywać wszelkie ewentualne naprawy. Zgłoszenie usterki lub awarii sprzętu następować będzie poczta elektroniczną lub telefonicznie. Czas reakcji serwisu Wykonawcy (rozpoczęcia czynności naprawczych) wynosić będzie 24 godziny licząc od momentu przyjęcia zgłoszenia o awarii (usterce). Czas ten nie uwzględnia sobót i dni ustawowo wolnych od pracy.
3. Okres gwarancji przedłuża się o czas naprawy przedmiotu zamówienia.

4. Wykonawca ponosi koszty dojazdów do czynności wykonywanych przez niego w okresie gwarancji.
5. Wykonawca zobowiązuję się do zapewnienia aktualizacji i wparcia technicznego w zakresie zakupionego oprogramowania w okresie 36 miesięcy od dnia podpisania bezusterkowego Protokołu odbioru przedmiotu zamówienia. W zakresie sprzętu Wykonawca udziela gwaranci na okres zgodny z OPZ.
6. Usługi gwarancyjne w zakresie oprogramowania świadczone będą w dni robocze w godzinach 8-16, z wyłączeniem dni ustawowo wolnych od pracy, a w przypadku awarii w trybie 24/7 365 dni w roku z czasem reakcji:
   1) przy awarii do 8h od momentu zgłoszenia;
   2) przy błędach do 12h roboczych od momentu zgłoszenia.

   Zgłoszenia o których mowa powyżej będą dokonywane na za pomocą aplikacji serwisowej udostępnionej pod adresem……. lub elektronicznie poprzez wysłanie zgłoszenia na adres …….., a w przypadku awarii poza godzinami i dniami roboczymi, telefonicznie pod numerem tel.: ……,
7. Czas reakcji w przypadku wystąpienia błędu oprogramowania wynosi 7 dni roboczych od przyjęcia zgłoszenia przez Wykonawcę, o której mowa w ust. 2 powyżej, a w przypadku awarii – Zamawiający jest zobowiązany do bezzwłocznej reakcji i eskalacji awarii bezpośrednio do Producenta/Dystrybutora oprogramowania.
8. Poprzez awarię Strony rozumieją krytyczny błąd oprogramowania bazodanowego lub operacyjnego powodujący, że nie jest możliwa jego eksploatacja lub jego istotnego obszaru z powodu uszkodzenia lub utraty: kodu programu, struktur danych, zawartości bazy danych, integralności danych.

§ 9
Zmiany Umowy

1. Wszelkie zmiany niniejszej Umowy, muszą być dokonane stosownym aneksem do Umowy sporządzonym w formie pisemnej, pod rygorem nieważności.
2. Z uwzględnieniem art. 455 ust.1 pkt 1 Ustawy zmiany Umowy są dopuszczalne w następujących okolicznościach:
   1) zmian wynikających z przekształceń własnościowych w przypadku połączenia,

przejęcia, wydzielenia, przekształcenia w inną formę organizacyjno-prawną,
2) zmian organizacyjno-technicznych, zmiany adresu, zmiany banku obsługującego Wykonawcę lub Zamawiającego,
3) zastąpienia przedmiotu Umowy w części lub w całości produktem o lepszych parametrach w porównaniu do parametrów określonych w ofercie, przy czym cena tego produktu nie może być wyższa niż cena oferowanego przedmiotu zamówienia,
4) zastąpienia sprzętu/oprogramowania, który ma być dostarczony w ramach realizacji niniejszej Umowy, sprzętem/oprogramowaniem nowym posiadającym co najmniej takie same parametry, jakie posiadał sprzęt/oprogramowanie będący podstawą wyboru oferty Wykonawcy w przypadku zakończenia produkcji lub wstrzymania produkcji sprzętu/oprogramowania, lub dystrybucji wyrobu będącego przedmiotem zamówienia, który ma być dostarczony, pod warunkiem, że Zamawiający zaakceptuje zmianę sprzętu/oprogramowania, a cena wprowadzonego sprzętu nie ulegnie zwiększeniu,
5) zmiany numerów katalogowych produktu, jeżeli Wykonawca zaoferuje przedmiot Umowy o tożsamych lub lepszych parametrach, nastąpi zmiana numerów katalogowych przez producenta przedmiotu Umowy,
6) zmiany terminu realizacji zamówienia w sytuacji, gdy zmiana ta wynika z przyczyn niezależnych od Wykonawcy, polegających w szczególności na: nieprzygotowaniu miejsca dostawy przez Zamawiającego w odpowiednim czasie, zmianie terminu dokonanej przez Zamawiającego z uwagi na nie dające się przewidzieć okoliczności, w przypadku siły wyższej polegającej w szczególności na powodzi, trzęsieniu ziemi, pożarze, wprowadzeniu stanu wyjątkowego bądź wojennego, wprowadzeniu przez odpowiednie organy lub trwaniu stanu zagrożenia epidemicznego bądź stanu epidemii mającego wpływ na termin realizacji zamówienia, niemożliwości przeprowadzenia szkolenia pracowników Zamawiającego z przyczyn leżących po stronie Zamawiającego w szczególności nieobecności spowodowanej chorobą osób szkolonych, opóźnieniu dostaw przez producenta z przyczyn leżących po stronie producenta,
7) ustawowej zmiany stawki podatku VAT, z przyczyn wynikających ze zmiany przepisów lub wprowadzonych drogą decyzji właściwych organów administracji państwowej,
8) sytuacji, których Zamawiający nie jest w stanie przewidzieć w chwili podpisania Umowy, a zmiana ta jest korzystna dla Zamawiającego lub leży w interesie publicznym,
9) zastąpienia dotychczasowego Wykonawcy nowym Wykonawcą - w wyniku sukcesji, wstępując w prawa i obowiązki Wykonawcy, w następstwie przejęcia, połączenia, podziału, przekształcenia, upadłości, restrukturyzacji, dziedziczenia lub nabycia dotychczasowego Wykonawcy lub jego przedsiębiorstwa, o ile

nowy Wykonawca spełnia warunki udziału w postępowaniu, nie zachodzą wobec niego podstawy wykluczenia oraz nie pociąga to za sobą innych istotnych zmian Umowy, a także nie ma na celu uniknięcia stosowania przepisów ustawy.

3. Żadna ze Stron Umowy nie będzie odpowiedzialna za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy spowodowane przez okoliczności traktowane jako Siła Wyższa.
4. Dla celów Umowy "Siła Wyższa" oznacza zdarzenie zewnętrzne, pozostające poza kontrolą Stron oraz niewiążące się z zawinionym działaniem Stron, którego Strony nie mogły przewidzieć i które uniemożliwia proces realizacji Umowy. Takie zdarzenia obejmują w szczególności: wojnę, rewolucję, pożary, powodzie, epidemie.
5. W przypadku zaistnienia Siły Wyższej, Strona, której taka okoliczność uniemożliwia lub utrudnia prawidłowe wywiązanie się z jej zobowiązań, niezwłocznie powiadomi drugą Stronę o takich okolicznościach i ich przyczynie (odpowiednio udokumentuje zaistniałe okoliczności). Wówczas Strony niezwłocznie ustalą zakres, alternatywne rozwiązanie i sposób realizacji Umowy. Strona zgłaszająca okoliczności musi kontynuować realizację swoich zobowiązań wynikających z Umowy w takim stopniu, w jakim jest to możliwe i musi szukać racjonalnych środków alternatywnych dla realizowania zakresu, jaki nie podlega wpływowi Siły Wyższej.
6. Jeżeli Siła Wyższa, będzie trwała nieprzerwanie przez okres 180 dni lub dłużej, Strony mogą w drodze wzajemnego uzgodnienia rozwiązać Umowę bez nakładania na żadną ze Stron dalszych zobowiązań oprócz płatności należnych z tytułu prawidłowo wykonanych usług.
7. Stan Siły Wyższej powoduje odpowiednie przesunięcie terminów realizacji Umowy chyba, że Strony postanowiły inaczej.

§ 10
Odstąpienie od Umowy

1. Odstąpienie od Umowy przez Zamawiającego może nastąpić w przypadku:
   1) dostarczenia przez Wykonawcę przedmiotu Umowy niezgodnego z ofertą,
   2) dostarczenia przedmiotu Umowy ze zwłoką przekraczającą 30 dni, niezależnie od możliwości naliczenia kar umownych,
2. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy lub dalsze wykonywanie Umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.
3. W przypadku odstąpienia od Umowy, o którym mowa w ust. 2, Wykonawca może

żądać jedynie wynagrodzenia za część Umowy wykonanej do dnia odstąpienia od Umowy.

4. Odstąpienie od Umowy winno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia.

§ 11
Kary umowne

1. W razie niewykonania lub nienależytego wykonania Umowy Wykonawca jest obowiązany zapłacić Zamawiającemu karę umowną w następujących przypadkach:
   1) w wysokości 20% łącznego wynagrodzenia brutto określonego w § 6 ust. 1, w przypadku odstąpienia przez Wykonawcę lub Zamawiającego od części lub całości Umowy lub innego sposobu rozwiązania Umowy z powodu okoliczności, za które Wykonawca ponosi wyłączną odpowiedzialność, w tym wskazanych w § 10 ust.1 pkt 1-2;
   2) w wysokości 0,1% łącznego wynagrodzenia brutto określonego w § 6 ust. 1, za każdy dzień zwłoki w przypadku nieterminowej realizacji zamówienia zgodnie z terminem określonym w § 5 ust. 1 niniejszej Umowy;
2. Zamawiający może dochodzić odszkodowania przewyższającego wysokość kar umownych, z zastrzeżeniem ust. 3.
3. Całkowita wzajemna odpowiedzialność odszkodowawcza Wykonawcy, bez względu na podstawę prawną roszczenia (tj. zarówno z tytułu niewykonania lub nienależytego wykonania Umowy, jak i z tytułu czynu niedozwolonego), ograniczona jest do wartości Umowy i nie obejmuje utraconych korzyści Zamawiającego.
4. Wykonawca zapłaci Zamawiającemu karę umowną za zwłokę w realizacji zobowiązań wynikających z gwarancji – w wysokości 100 zł, za każdy rozpoczęty dzień zwłoki w zakresie realizacji gwarancji.
5. Łączna wysokość kar umownych naliczonych na podstawie § 11 ust. 1 nie może przekroczyć 20 **%** łącznej wartości Umowy brutto określonej w § 6 ust. 1 Umowy.
6. Naliczenie kar umownych nie wyłącza prawa dochodzenia odszkodowania na zasadach ogólnych jeżeli wielkość szkody przekracza wysokość naliczonych kar umownych.

§ 12
Podwykonawcy

Wykonawca oświadcza, że przedmiot zamówienia wykona własnymi siłami z/ bez udziału podwykonawców/z udziałem podwykonawców*tj. ……

§ 13
Postanowienia końcowe

1. Umowa obowiązuje z dniem podpisania.
2. Zmiany niniejszej Umowy i wynikające z realizacji niniejszej Umowy wymajają formy pisemnej pod rygorem nieważności. Za skuteczne doręczenie oświadczenia zostanie uznane również przekazanie drugiej stronie pisma lub informacji w formie pisemnej, osobiście bądź też pocztą elektroniczną wyznaczonemu do koordynacji przedmiotu Umowy przedstawicielowi.
3. Strony postanawiają, że Wykonawca nie ma prawa dokonywać czynności skutkujących bezpośrednim lub pośrednim przeniesieniem wynikających z niniejszej Umowy wierzytelności przysługujących Wykonawcy w stosunku do Zamawiającego bez jego pisemnej zgody, pod rygorem nieważności, w szczególności Wykonawca nie ma prawa bez zgody Zamawiającego dokonywać przelewu wierzytelności ani ustanawiać ograniczonych praw rzeczowych na wierzytelnościach. Dokonanie ww. czynności bez zgody Zamawiającego będzie skutkować rozwiązaniem Umowy w trybie natychmiastowym i obowiązkiem zapłaty przez Wykonawcą na rzecz Udzielającego Zamówienie kary umownej w wysokości równowartości przeniesionej/obciążonej wierzytelności.
4. Spory powstałe na tle realizacji niniejszej Umowy strony poddają pod rozstrzygnięcie sądu właściwego dla siedziby Zamawiającego.
5. W sprawach nieuregulowanych w niniejszej umowie będą miały zastosowanie właściwe przepisy Kodeksu Cywilnego oraz ustawy z dnia 19 września 2019 r. Prawo Zamówień Publicznych, SWZ oraz oferta Wykonawcy.
6. Załączniki do Umowy stanowią integralną część Umowy.
7. Umowę niniejszą sporządzono w dwóch jednobrzmiących egzemplarzach, oba na prawach oryginału, po jednym dla każdej ze Stron.

WYKONAWCA ***ZAMAWIAJĄCY***

Załączniki do umowy:

1) Załącznik nr 1 – Opis przedmiotu zamówienia
2) Załącznik nr 2 – Formularz oferty

DOLNOŚLASKIE CENTRUM LECZENIA UZALEŻNIEŃ
W CZARNYM BORZE

58-379 Czarny Bór, ul. Parkowa 8

tel. (74) 84 50 125, fax (74) 84 50 290, e-mail: sekretariat@dclu.pl www.dclu.pl

Jednocześnie Zamawiający informuje, że w wyniku dokonanych zmian dokonał zmiany treści ogłoszenia o zamówieniu.

Signature Not Verified

Dokument podpisany
przez Marek Zawada
Data: 2023.10.18
10:07:46 CEST