Przedmiotem zamówienia jest dostawa i wdrożenie systemu bezpieczeństwa dla potrzeb zabezpieczeń Zamawiającego w kontekście wymagań RODO.

Szczegółowy opis przedmiotu zamówienia:

1. **Zapora sieciowa**

LP	Opis funkcjonalny
1.	Zapora musi być dostarczona w postaci dedykowanego urządzenia sieciowego wraz z zainstalowanym systemem operacyjnym i oprogramowaniem, pochodzących od jednego producenta.
2.	Urządzenie musi mieć możliwość pracy z drugim oraz trzecim takim samym urządzeniem w trybie klastra wysokiej dostępności (aktywny/pasywny) oraz w trybie klastra z równoważeniem obciążeń (aktywny/aktywny).
3.	Musi istnieć wspierana przez producenta możliwość uruchomienia tego samego oprogramowania zapory z takimi samymi funkcjonalnościami i systemem operacyjnym jak na dostarczonym dedykowanym urządzeniu na ogólnie dostępnej platformie INTEL x86 (w ramach listy kompatybilności producenta).
4.	Zapora musi posiadać wydajność co najmniej 4 Gbps ruchu poddawanego inspekcji przez mechanizmy zapory sieciowej oraz posiadać wydajność 1,5 Gbps ruchu szyfrowanego VPN.
5.	Zapora musi obsługiwać co najmniej 3 miliony jednoczesnych sesji/połączeń.
6.	Zapora ma posiadać co najmniej 6 fizycznych interfejsów 10/100/1000 Ethernet.
7.	Zapora ma posiadać dedykowane dla zarządzania porty, minimum port konsoli oraz minimum 1 dysk twardy o pojemności minimum 300 GB. System zabezpieczeń zapory musi być oparty na technologii Statefull Inspection oraz Application Level Gateway. System zabezpieczeń zapory umożliwia ochronę sieci bez ograniczeń dla liczby adresów IP.
8.	Zapora sieciowa musi być zarządzana przez zewnętrzny system zarzadzania opisany w punkcie 2 niniejszego opisu przedmiotu zamówienia.
9.	Polityka bezpieczeństwa zapory w zakresie kontroli ruchu sieciowego uwzględnia kierunek przepływu pakietów, protokoły i usługi sieciowe, użytkowników i serwery usług, stan połączenia oraz dane aplikacyjne (m.in. obsługuje fragmentację IP, ochronę systemu operacyjnego przed atakami Exploit i DoS).
10.	Zapora wykonuje dynamiczną i statyczną translację adresów NAT. Reguły NAT są generowane automatycznie lub definiowane ręcznie.
11.	Komunikacja pomiędzy modułem zapory sieciowej i systemem zarządzania jest szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych generowanych przez system zarządzania.
12.	Komunikacja pomiędzy interfejsem GUI administratora i systemem zarządzania jest szyfrowana.
13.	Uwierzytelnianie administratorów zapory odbywa się za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych. Istnieje możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników).
14.	Zapora posiada wiele metod uwierzytelniania użytkowników lokalnych i zdalnych (np. uwierzytelnianie przezroczyste gdzie Firewall przechwytuje sesję i uwierzytelnia jej użytkownika, uwierzytelnianie za pomocą agenta na stacji użytkownika, uwierzytelniania po połączeniu się z modułem Firewall). Baza użytkowników jest przechowywana lokalnie na Firewall lub na zewnętrznym serwerze (np. LDAP).
15.	Funkcjonalność zabezpieczeń zapory musi zapewniać ochronę przez intruzami (IPS). Mechanizm musi zapewniać co najmniej wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan). Aktualizacja bazy sygnatur ma się odbywać poprzez sieć, na żądanie administratora.
16.	Zapora sieciowa musi umożliwiać kontrolę aplikacji sieciowych używanych przez użytkowników wewnętrznych. Identyfikacja aplikacji ma odbywać się w oparciu o bazę danych utrzymywaną przez producenta rozwiązania.
17.	Zapora sieciowa musi umożliwiać filtrowanie URL. Identyfikacja URL ma odbywać się w oparciu o bazę danych utrzymywaną przez producenta rozwiązania.
18.	Zapora sieciowa musi umożliwiać skanowanie antywirusowe minimum protokołów HTTP, HTTPS, FTP, SMTP, POP3.
19.	Zapora sieciowa musi posiadać moduł umożliwiający identyfikację stacji roboczych użytkowników zainstalowanych w sieci wewnętrznej, które są zainfekowane agentami botnet.
20.	Zapora sieciowa musi posiadać moduł antyspamowy umożliwiający kontrolę protokołów SMTP i

	POP3.
21.	Zapora sieciowa musi umożliwiać rozszerzenie o następujące funkcjonalności: a) Moduł ochrony przez zagrożeniami typu zero-day analizujący zachowanie plików w środowisku wirtualnym (Sandboxing). b) Moduł eliminujący z dokumentów elementy aktywne będące potencjalnym nośnikiem wirusów (makrodefinicje, aplety, akcje audio lub wideo). W szczególności moduł musi umożliwiać przekształcenie dokumentów typu Microsoft Word zawierających elementy aktywne w nieedytowalny plik typu pdf a także zapewniać usuwanie ataków typu zero-day, za pomocą rekonstrukcji dokumentów do formatu bezpiecznego (pozbawionego elementów programistycznych), c) Moduł umożliwiający wykrywanie wycieku danych (DLP) Dodatkowe moduły (pkt. a, b, c) muszą pochodzić od producenta urządzenia.
22.	Zapora umożliwia tworzenie sieci VPN w oparciu o standard IPSec/IKE, funkcjonujące w trybie site-site oraz client-site. Funkcjonalność klienta VPN może zostać rozszerzona o zarządzany centralnie Personal Firewall oraz o możliwość sprawdzenia konfiguracji zdalnego PC przed nawiązaniem sesji VPN.
23.	Uwierzytelnianie w sieci VPN odbywa się za pomocą certyfikatów cyfrowych wydawanych lokalnie oraz w razie potrzeby przez zewnętrzny urząd certyfikacji.
24.	Zabezpieczenie danych w sieci VPN odbywa się z użyciem mocnych algorytmów kryptograficznych (m.in. AES-256).
25.	Zapora musi umożliwiać jednoczesne uruchomienie trybu L2 (bridge, transparent) i trybu L3 (routing) w ramach tego samego jednego urządzenia fizycznego i jednego systemu wirtualnego.
26.	Zapora zapewnia uruchomienie oprogramowania zapory (z ew. dokupieniem innego rodzaju licencji) na wszystkich następujących platformach: urządzeniach typu appliance dostarczanych przez producenta, bezpośrednio na platformie sprzętowej zgodnej z Intel x86, jako maszyny wirtualnej w środowiskach VMware, Hyper-V oraz KVM.
27.	Wsparcie producenta dla zapory obejmujące aktualizacje oprogramowania wbudowanego oraz sygnatur – minimum 1 rok.
28.	Gwarancja minimum 1 rok.
29.	Wykonawca zainstaluje i wdroży dostarczoną zaporę w sieci Zamawiającego zgodnie z dokumentacją producenta.

2. Zewnętrzny systemem zarządzania zaporą

LP	Opis funkcjonalny
1.	System umożliwia zarządzanie dostarczaną zaporą - poprzez zarządzanie należy rozumieć konfigurację polityki bezpieczeństwa (polityka firewall, VPN, polityka ochrony antywirusowej, antyspamowej, ochrony przed atakami sieciowymi), zarządzanie kontami administratorów i użytkowników, obsługę zdarzeń generowanych przez moduły zapór sieciowych.
2.	System zarządzania musi być dostarczany przez producenta zapory.
3.	System posiada wewnętrzny, zintegrowany urząd certyfikacji (Certificate Authority).
4.	System jest obsługiwany za pomocą konsoli użytkownika, która musi być dostarczona w postaci dedykowanej graficznej konsoli administratora (GUI) działającej pod systemem operacyjnym Windows. Konsola zarządzania posiada możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.
5.	Komunikacja pomiędzy zaporą sieciowa i systemem zarządzania jest szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych generowanych przez system zarządzania.
6.	Komunikacja pomiędzy interfejsem GUI konsoli administratora a systemem zarządzania jest szyfrowana.
7.	Uwierzytelnianie administratorów odbywa się za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych. Istnieje możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników).
8.	System zarządzania jest w stanie wyświetlić z graficznej konsoli listę aktywnych połączeń obsługiwanych przez moduły zapór sieciowych. Informacja o połączeniu powinna zawierać minimum adres źródła, adres przeznaczenia, port źródła, port przeznaczenia oraz identyfikator usługi sieciowej.
9.	System zarządzania umożliwia wyszukiwanie i filtrację zdarzeń wygenerowanych przez moduły zabezpieczeń. Administrator jest w stanie zdefiniować własne szablony wyszukiwania i wyświetlania zdarzeń.

10.	System umożliwia monitorowanie i prezentowanie za pomocą graficznej konsoli takich parametrów sprzętowych zarządzanych zapór sieciowych jak: średnie obciążenie procesora, zajętość pamięci operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa.
11.	System umożliwia graficzne wyświetlanie statystyk ruchu sieciowego, przetwarzanego przez zapory sieciowe, takich jak: najczęściej wykorzystywane usługi sieciowe, najczęstsze źródła transmisji, najczęstsze adresy docelowe, aktywne i zerwane tunele VPN.
12.	System zarządzania umożliwia integrację z usługą katalogową LDAP, w szczególności z Microsoft Active Directory. Integracja ma co najmniej polegać na możliwości zaimportowania grup użytkowników z LDAP oraz wykorzystywanie tych grup w regułach polityki bezpieczeństwa.
13.	System zarządzania zapewnia uruchomienie (tego samego oprogramowania, z ew. dokupieniem licencji) na wszystkich wymienionych platformach: urządzeniach typu appliance dostarczanych przez producenta, systemie Windows, systemie Linux, bezpośrednio na platformie sprzętowej zgodnej z Intel x86, jako maszyny wirtualnej w środowiskach VMware, Hyper-V oraz KVM.
14.	System zarządzania zapewnia zarządzanie polityką bezpieczeństwa wszystkich elementów zapory z dedykowanej aplikacji dla Windows, bez konieczności używania protokołów https/https, komunikującej się z systemem zarządzania w sposób szyfrowany.
15.	System zarządzania realizuje czasowe lub stałe, natychmiastowe zablokowanie wskazanego połączenia bezpośrednio z graficznego monitora połączeń, bez konieczności modyfikowania polityki bezpieczeństwa.
16.	System bezpieczeństwa zapewnia wyświetlanie, bezpośrednio w graficznym widoku polityki bezpieczeństwa, licznika trafień dla każdej z reguł.
17.	Zewnętrzny system zarządzania zostanie zainstalowany na serwerze posiadanym przez Zamawiającego.
18.	Zewnętrzny system zarządzania będzie umożliwiał zarządzanie minimum 3 urządzeniami typu zapora sieciowa.
19.	Wsparcie producenta dla zewnętrznego systemu zarządzania obejmujące aktualizacje oprogramowania – minimum 1 rok.
20.	Wykonawca zainstaluje i wdroży dostarczony system zarządzania i podłączy do niego dostarczona zaporę sieciową.

3. System kopii zapasowej (backupu)

Wymagania podmiotowe:

a) Wykonawca musi dysponować minimum 1 osobą posiadającą certyfikat Arcserve UDP High Availability Master Engineer wystawiony przez firmę Arcserve.
b) Wykonawca przed podpisaniem umowy dostarczy kopię tego certyfikatu poświadczoną za zgodność z oryginałem przez Wykonawcę.
c) Zamawiający zastrzega sobie prawo do weryfikacji autentyczności certyfikatu w firmie Arcserve.

Rozwiązanie musi być dostarczone w formie oprogramowania, które musi spełniać następujące kryteria:

LP	Opis funkcjonalny
1.	Być licencjonowane wieczyście dla 4 serwerowych gniazd fizycznych obsadzonych procesorami z możliwością uruchomienia wszystkich opisanych funkcjonalności, dla serwerów fizycznych, nielimitowanej liczby serwerów wirtualnych, nielimitowanej liczby baz i aplikacji oraz nielimitowanej ilości danych.
2.	Odczytywać kopie zapasowe wykonane za pomocą posiadanego przez Zamawiającego oprogramowania Arcserve UDP.
3.	Zarządzanie z posiadanego przez Zamawiającego serwera zarządzania backupem Arcserve UDP w zakresie wymienionych w Opisie przedmiotu zamówienia funkcji backupu.
4.	Posiadać, opisane w dokumentacji produktu, wsparcie producenta oprogramowania na instalację systemu zarządzania nim na platformie wirtualnej.
5.	Zapewniać utworzenie repozytorium backupu, tj. wykonywanie backupu bezpośrednio na dyskach lokalnych (DAS), dyskach przenośnych, macierzach dyskowych SAN i NAS, jak również w chmurze.
6.	Wykonywać backup bezpośrednio do repozytorium oparty o technologię przyrostowej kopii migawkowej na poziomie bloków danych, to znaczy – tylko pierwszy backup jest pełny, pozostałe

	wieczyście tylko przyrostowe (bez konieczności wykonywania ponownie kopii pełnych), dla serwerów fizycznych i wirtualnych
7.	Licencja na oprogramowanie musi umożliwiać pełny dostęp dla użytkowników do udokumentowanego przez producenta API dostępnego przez protokoły http i https.
8.	Wsparcie dla systemów operacyjnych systemów fizycznych i wirtualnych oraz powiadamianie o zdarzeniach.
9.	Możliwość backupu danych (wybrane pliki, całe systemy, serwery wirtualne, aplikacje) bezpośrednio na taśmę.
10.	Możliwość backupu danych (wybrane pliki, całe systemy, serwery wirtualne, aplikacje) na zasób dyskowy a następnie ręcznie i automatycznie na taśmę.
11.	Możliwość wykonywania backupu na współdzieloną bibliotekę taśmową poprzez sieć SAN.
12.	Możliwość backupu zasobów macierzy dyskowych przy użyciu protokołu NDMP.
13.	Możliwość wykonania backupu aplikacji działających w systemach MS Windows: a) Exchange 2010, 2013 b) MS SQL / SQL Express 2012, 2014, 2016 c) Oracle 10.x, 11.x, 12c
14.	Możliwość wykonania backupu całego serwera wirtualnego lub fizycznego, dla systemów operacyjnych MS Windows: 2012R2, 2016 niezależnie od zainstalowanych aplikacji, z zapewnieniem następujących funkcjonalności: a) backup jest wykonywany w formie maszyny wirtualnej na serwerze Microsoft Hyper-V lub VMware vSphere, z możliwością natychmiastowego uruchomienia, bez konieczności wykonywania dodatkowych procesów na plikach backupu b) możliwość monitorowania statusu backupu z konsoli zarządzającej c) backup w trybie ciągłym, bez określania przedziałów czasowych pomiędzy kolejnymi backupami, a jedynie określenia z jakiego czasu mają być dostępne kopie zapasowe d) możliwość odtworzenia aplikacji z dowolnego punktu na osi czasu, ze zdefiniowanego okresu czasu, z którego są przechowywane kopie zapasowe. e) możliwość odtworzenia całego zabezpieczanego systemu w trybie Bare Metal Recovery, bez konieczności wcześniejszej instalacji systemu operacyjnego i sterowników f) możliwość uruchomienia kopii zapasowej w sposób zapewniający konsystencję danych aplikacji, w sposób automatyczny po wykryciu awarii systemu zabezpieczanego, lub ręczny w dowolnym momencie. g) możliwość wykonania testów poprawności działania backupu polegających na uruchomieniu zapasowej maszyny wirtualnej zabezpieczanego systemu w sposób umożliwiający wykonanie testów poprawności działania systemu i aplikacji na nim zainstalowanych (np. zalogowanie się do maszyny wirtualnej, uruchomienie skryptów testowych, wykonanie normalnych operacji administratora i użytkownika na serwerze i aplikacji), bez przerywania wykonywania backupu i bez konieczności wykonywania jakichkolwiek operacji na zabezpieczanym systemie (w szczególności jego zatrzymania lub wyłączenia) h) i) możliwość wykonania w/w testów w sposób ręczny na żądanie, jak również w sposób w pełni automatyczny, według terminarza, z generowaniem reportu o wynikach testów.
15.	Wsparcie techniczne producenta z prawem do pobierania i instalacji nowych wersji oprogramowania przez min. 1 rok.
16.	Wykonawca zainstaluje i wdroży dostarczone oprogramowanie do backupu. Wykonawca wykona rekonfigurację posiadanego przez Zamawiającego oprogramowania Arcserve do współpracy z dostarczonym oprogramowaniem do backupu w sposób zapewniający pracę zgodnie z wymaganiami Opisu przedmiotu zamówienia. Prace będzie wykonywała osoba posiadająca certyfikat Arcserve wymagany w SIWZ.

4. System silnego uwierzytelniania

System silnego uwierzytelniania musi spełniać wszystkie poniższe wymagania:

LP	Opis funkcjonalny
1.	System uwierzytelniania musi być zbudowany w oparciu o rozwiązanie programowe, tj. oprogramowanie serwera uwierzytelniającego oraz zintegrowane z nim urządzenia uwierzytelniające.
2.	System musi posiadać możliwość obsługi – równoczesnego uwierzytelniania minimum 25 użytkowników z możliwością rozbudowy.
3.	Serwer uwierzytelniania musi umożliwiać instalację na systemach operacyjnych: Windows Server

	2012, 2012 R2, 2016, RHEL 6.x, 7.x, SLES 12.
4.	System uwierzytelniania musi zapewniać wsparcie producenta dla instalacji serwera uwierzytelniania na wirtualnych systemach operacyjnych, uruchomionych w środowisku wirtualizującym: VMware/ESX 4, 5, 6, MS Hyper-V 2012, 2012 R2, 2016, RHEL 6.x, 7.x.
5.	System uwierzytelniania musi umożliwiać uruchomienie w oparciu o serwery aplikacji Java: Apache Tomcat Application Server 8.5.11 lub nowszy, IBM WebSphere 8.5.5, 9.0, Oracle WebLogic 12c, 12cR2.
6.	System uwierzytelniania musi umożliwiać jednoczesne utworzenie wielu różnych repozytoriów do przechowywania danych kont użytkowników, co najmniej w bazach danych: PostgreSQL 9.3, 9.4, 9.5, Microsoft SQL Server 2012, 2012 R2, 2014, 2016, Oracle Database 11g R1, 11g R2, 12c, DB2 Universal 10.5, 11.1, MySQL 5.5, 5.6, 5.7.
7.	System uwierzytelniania musi umożliwiać jednoczesne utworzenie wielu różnych repozytoriów do przechowywania danych kont użytkowników, co najmniej w usługach katalogowych: IBM Tivoli Directory Server 6.3, 6.4, Novell eDirectory 8.8.7, 8.8 SP, Oracle Enterprise Directory Server 6.3 (SunONE), Oracle Internet Directory 11g R2, Microsoft Active Directory 2012, 2012 R2, 2016, Microsoft Active Directory Lightweight Directory Services 2012, 2012 R2, 2016, OpenLDAP 2.4
8.	Serwer uwierzytelniania musi udostępniać udokumentowane przez producenta API, dostępne przez http/https.
9.	Serwer uwierzytelniania musi umożliwiać uwierzytelnianie użytkowników dostępu zdalnego do systemów wymienionych poniżej producentów, udokumentowane przez producenta oprogramowania do uwierzytelniania: Cisco, Citrix, Check Point, F5, Juniper, Microsoft, Dell
10.	Serwer uwierzytelniania musi umożliwiać uwierzytelnianie aplikacji zewnętrznych za pośrednictwem wtyczki Radius PAM.
11.	Serwer uwierzytelniania musi posiadać zintegrowany własny serwer Radius
12.	Serwer uwierzytelniania musi umożliwiać integrację jego logowania wieloskładnikowego, za pomocą udokumentowanego przez producenta API, z własnymi aplikacjami użytkownika dla platform programistycznych: Java, .Net.
13.	Serwer uwierzytelniania musi obsługiwać następujące metody silnego logowania i logowania wieloskładnikowego: a) Nazwa użytkownika i hasło b) Hasła jednorazowe generowane za pomocą tokenów sprzętowych i programowych c) Hasła jednorazowe z predefiniowanej listy haseł d) Hasła jednorazowe generowane za pomocą tabeli (Grid) e) Autentykacja na podstawie bazy wiedzy (predefiniowane pytania i odpowiedzi) f) Autentykacja typu out-of-band, za pomocą: kodów jednorazowych przesyłanych drogą mailową, kodów jednorazowych przesyłanych przez SMS, komunikacji głosowej, g) Autentykacja dwustronna, wzajemna w tym samym czasie (mutual Authentication) h) Autentykacja urządzenia, z którego jest wykonywania autentykacja na podstawie unikalnego profilu urządzenia utworzonego przy wykorzystaniu minimum następujących elementów (jednego lub wielu w dowolnej kombinacji): adres sprzętowy karty sieciowej (MAC), system operacyjny (wersja, poziom service pack, wersja poprawek), informacje o procesorze (ID, wersja), informacje o systemie (producent, model, wersja) oraz informacje o urządzeniach w nim zainstalowanych (karty sieciowe, karty graficzne, dyski twarde, napędy CD/DVD), przeglądarka internetowa (nazwa przeglądarki, wersja).
14.	Serwer musi umożliwiać zarządzanie autentykacją sposób umożliwiający konfigurację sposobów silnego uwierzytelniania dla użytkowników z uwzględnieniem: a) Przydziału użytkownika do grupy b) Systemu/aplikacji, do którego użytkownik się loguje c) Urządzenia/komputera, z którego użytkownik się loguje d) Urządzenia/programu, który jest używany do uwierzytelniania wieloskładnikowego
15.	Możliwość obsługi tokenów programowych na platformach systemowych: Windows 7, Windows 8, Windows 10, Windows 2012 R2, Mac OS X, Google Android, Apple iOS, Java Phone zgodny z MIDP.
16.	System musi mieć możliwość rozbudowy o funkcję umożliwiającą dokonywania lokalizacji użytkownika (kraj, miasto), określonej na podstawie adresu IP systemu, z którego jest wykonywane logowanie (baza lokalizacyjna jest dostarczana w formie subskrypcji przez producenta oprogramowania do silnego uwierzytelniania).
17.	Możliwość rozszerzenia funkcjonalności oprogramowania – przez dodanie licencji producenta w ramach tego samego produktu - o funkcje: a) Zarządzanie certyfikatami cyfrowymi X.509 (przydzielanie, konfigurowanie), z możliwością zarządzania CA Microsoft

	b) Wykorzystanie certyfikatów cyfrowych do silnego uwierzytelniania, z możliwością wykorzystania certyfikatów cyfrowych, składowanych na: lokalnych systemach, standardowych SmartCard'ach, tokenach USB, aplikacji mobilnej umożliwiającej użycie certyfikatów przez łącze Bluetooth i NFC, zainstalowanej na mobilnych systemach operacyjnych: Google Android, Apple iOS.
18.	Możliwość rozbudowy o dodatkowe serwery uwierzytelniania umożliwiające: a) Pracę w trybie wysokiej dostępności – jedne serwer główny i wiele serwerów zapasowych. Musi być możliwość uruchomienia serwerów zapasowych na innym systemie operacyjnym niż serwer główny, np. (np. serwer główny na platformie Linux, jeden serwer zapasowy na platformie Windows a drugi zapasowy na Solaris) b) Pracę w trybie współdzielenia obciążeń – każdy z serwerów jednocześnie obsługuje żądania uwierzytelnienia dla tych samych repozytoriów użytkowników. Musi być możliwość uruchomienia każdego z tych serwerów uwierzytelniania na innym systemie operacyjnym c) c) Możliwość rozbudowy o system samoobsługi użytkownika, pochodzący od tego samego producenta, w pełni integrujący się z systemem silnego uwierzytelniania
19.	Oprogramowanie typu Soft Token – tokeny programowe dla 5 użytkowników zapewniające działanie i wsparcie producenta. Tokeny programowe muszą być dostarczane przez tego samego producenta co oprogramowanie do silnego uwierzytelniania,
20.	Licencja na System silnego uwierzytelnia musi zapewniać prawo do pobierania nowych wersji oprogramowania i poprawek przez minimum 1 rok
21.	System silnego uwierzytelniania zostanie zainstalowany na sprzęcie i systemie operacyjnym posiadanym przez Zamawiającego.
22.	Wykonawca wdroży i zintegruje dostarczony system silnego uwierzytelniania z dostarczoną zaporą sieciową (uwierzytelnianie do VPN).