Załącznik nr 9 do SIWZ – Opis środków organizacyjno-technicznych, wyposażenia zakładu i urządzeń technicznych

Nr referencyjny nadany sprawie przez Zamawiającego: **TARRSA/IT/1/2019**

**Opis środków organizacyjno-technicznych,**

**wyposażenia zakładu i urządzeń technicznych**

Postępowanie pn.„Usługi zapewnienia dostępu do infrastruktury informatycznej

w modelu usługowym wraz z usługami uzupełniającymi i obsługą informatyczną”

**WYKONAWCA:**

……………………………………..

……………………………………..

(*(pełna nazwa/firma, adres)*

Brak odpowiedzi w którejkolwiek z obligatoryjnych części lub ich modyfikacja w taki sposób, że zostaną one usunięte – będzie skutkować uznaniem przez Zamawiającego, że Wykonawca nie wykazał spełnienia warunków udziału w Postępowaniu, a co za tym idzie podlega wykluczeniu na podstawie art. 24 ust. 1 pkt. 12) Ustawy Pzp.

|  |
| --- |
| 1. ŚRODKI TECHNICZNE I ORGANIZACYJNE W ZAKRESIE OGÓLNEGO ROZPORZĄDZENIA W ZAKRESIE DANYCH OSOBOWYCH |
| Wykonawca, **a w przypadku Wykonawców wspólnie ubiegających się o zamówienie każdy** **z nich**, zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi 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) ) i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz chroniło prawa osób, których dane dotyczą.  TAK\* ☐ NIE\* ☐  *\*zaznaczyć właściwe* |
| 1. WYMAGANIA DLA OŚRODKA CENTRUM PRZETWARZANIA DANYCH (CPD) |
| Podstawa dysponowania ośrodkiem centrum przetwarzania danych: ………………………………………  Ośrodek przetwarzania posiada zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo danych przetwarzanych. Ośrodek ponosi odpowiedzialność w zakresie bezpieczeństwa informacji przechowywanych na wykorzystanej infrastrukturze serwerowej.   |  |  |  |  | | --- | --- | --- | --- | | 1. OBIEKT I LOKALIZACJA | | | | | L.p. | Parametr lub kryterium | Wyeliminowanie zagrożenia | Wykonawca spełnia  (TAK / NIE) | | 1 | Centrum przetwarzania danych zlokalizowane na terenie na terenie UE lub Lichtenstainu, Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na terenie Polski lub UE. | Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR. |  | | 2 | Ogrodzony teren centrum przetwarzania danych. | Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka. |  | | 3 | Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie. | Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury. |  | | 4 | Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej | Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych. |  | | 5 | Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych. | Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko). |  | | 6 | Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób). | Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń. |  | | 7 | Minimum 200 m oddalenie od linii wysokiego napięcia i elektrowni. | Zagrożenie spowodowania uszkodzeń wynikających z awarii linii wysokiego napięcia, ryzyko wybuchów, ryzyko pożarów. Zagrożenie długotrwałego ograniczenia dostępu do ośrodka wynikającego z wykonywanych napraw. |  | | 8 | Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami. | Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności). |  | | 9 | Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Zamawiającemu od źródeł pól zakłócających (transformatory SN i WN). | Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pół zakłócających pracę urządzeń elektrycznych i magnetycznych. |  | | 10 | Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu | Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych. |  | | 11 | Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m | Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych. |  | | 12 | Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1. | Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych. |  | | 13 | Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej. | Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej. |  | | 1. WĘZŁY TELEKOMUNIKACYJNE | | | | | 1 | Podłączenie w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym | Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora. |  | | 2 | Dojścia połączeń do ośrodka wykonane dwoma niezależnymi trasami kablowymi. | Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem. |  | | 3 | Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP | Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet. |  | | 4 | Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99% | Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet. |  | | 5 | Węzeł telekomunikacyjny wyposażony w redundantny system firewall | Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej. |  | | 6 | Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci. | Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy. |  | | 1. ZASILANIE | | | | | 1 | Dostępność roczna systemu zasilania 99,99% | Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń. |  | | 2 | Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT | Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania. |  | | 3 | System zasilania awaryjnego UPS osobno na każdą linię zasilającą | Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego. |  | | 4 | Redundantny system agregatów prądotwórczych | Zagrożenie braku zachowania zasilania |  | | 5 | System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną | Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów. |  | | 6 | Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy. | Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów. |  | | 1. BEZPIECZEŃSTWO | | | | | 1 | Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 dni, system kontroli dostępu (SKD). | Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urządzeń. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urządzeń. |  | | 2 | Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania. | Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu. |  | | 3 | Ochrona przez zewnętrzną licencjonowaną firmę. | Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej. |  | | 4 | System CCTV zapewnia ciągły 365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne. | Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób. |  | | 5 | System CCTV powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres co najmniej 21 dni. | Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń. |  | | 6 | System SKD dzieli centrum przetwarzania danych wraz z terenem na minimum IV strefy dostępu z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku. |  | | 7 | Dostęp do strefy I (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów). | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |  | | 8 | Dostęp do strefy II (część administracyjno-biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |  | | 9 | Dostęp do strefy III (strefa technologiczna) możliwy wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |  | | 10 | Dostęp do strefy IV (pomieszczenia ze sprzętem komputerowym Zamawiającego) możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |  | | 11 | System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego. | Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia. |  | | 12 | Ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej. | Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru. |  | | 1. MONITOROWANIE | | | | | 1 | System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7 | Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej. |  | | 2 | Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności. | Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń. |  | | 1. BEZPIECZEŃSTWO SPRZĘTU INFORMATYCZNEGO | | | | | 1 | Izolacja sprzętu krytycznego | |  | | 2 | Ochrona przed uszkodzeniem | |  | | 3 | Rejestr wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego | |  | | 4 | Ochrona przed dostępem dla osób nieupoważnionych | |  | | 1. NAPRAWY I KONSERWACJA SPRZĘTU | | | | | 1 | Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu. | |  | | 2 | Obsługa i naprawy muszą być dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami Ośrodka. | |  | | 3 | Należy usuwać nośniki danych przed przekazaniem sprzętu do naprawy. | |  | | 4 | Należy stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi). | |  | | 5 | Należy wykonywać przeglądy techniczne zgodnie z wymaganiami producenta sprzętu i procedurami wewnętrznymi Ośrodka. | |  | | 6 | Należy chronić Zamawiającego przed instalacją złośliwego oprogramowania. | |  | | 7 | Należy prowadzić rejestr incydentów, awarii i usterek. | |  | | 8 | Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu. | |  | |
| *\*w każdym wierszu wpisać odpowiednio TAK – jeśli spełniony jest wymóg lub NIE - jeśli wymóg nie jest spełniony* |
| 1. PARAMETRY TECHNICZNE SERWERÓW WIRTUALNYCH |
| Podstawa dysponowania ośrodkiem centrum przetwarzania danych: ………………………………………   |  |  |  |  | | --- | --- | --- | --- | | 1 | Serwery (www) x 1 | Minimalne wymagania Zamawiającego | Warunki oferowane przez Wykonawcę | | a | Architektura | x86-64 |  | | b | Pamięć podstawowa | 4 GB DDR3 1333MHz |  | | c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |  | | d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |  | | e | Interfejsy sieciowe | 2 x 1Gb |  | | f | Moduł zarządzania | Wymagany |  | | g | System operacyjny | CentOS z możliwością upgrade do nowszej wersji lub równoważny |  | | h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |  | | i | Adres zewnętrzny | 3 x IPv4 |  | | 2 | Serwery (plików) x 2 | Minimalne wymagania Zamawiającego |  | | a | Architektura | x86-64 |  | | b | Pamięć podstawowa | 4 GB DDR3 1333MHz |  | | c | Procesor/Procesory | 4 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |  | | d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |  | | e | Interfejsy sieciowe | 2 x 1Gb |  | | f | Moduł zarządzania | Wymagany |  | | g | System operacyjny | Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny |  | | h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |  | | i | Przestrzeń dyskowa | 3000 GB (5.000 IOPS) |  | | 3 | Serwery (aplikacja) x 2 | Minimalne wymagania Zamawiającego |  | | a | Architektura | x86-64 |  | | b | Pamięć podstawowa | 4 GB DDR3 1333MHz |  | | c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |  | | d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |  | | e | Interfejsy sieciowe | 2 x 1Gb |  | | f | Moduł zarządzania | Wymagany |  | | g | System operacyjny | Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny |  | | h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |  | | 4 | Serwery (generator) x2 | Minimalne wymagania Zamawiającego |  | | a | Architektura | x86-64 |  | | b | Pamięć podstawowa | 2 GB DDR3 1333MHz |  | | c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |  | | d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |  | | e | Interfejsy sieciowe | 2 x 1Gb |  | | f | Moduł zarządzania | Wymagany |  | | g | System operacyjny | CentOS z możliwością upgrade do nowszej wersji lub równoważny |  | | h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |  | | 5 | Serwery (AD) x 2 | Minimalne wymagania Zamawiającego |  | | a | Architektura | x86-64 |  | | b | Pamięć podstawowa | 4 GB DDR3 1333MHz |  | | c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |  | | d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |  | | e | Interfejsy sieciowe | 2 x 1Gb |  | | f | Moduł zarządzania | Wymagany |  | | g | System operacyjny | Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny |  | | h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |  | | 6 | Serwery (OCS) x 1 | Minimalne wymagania Zamawiającego |  | | a | Architektura | x86-64 |  | | b | Pamięć podstawowa | 2 GB DDR3 1333MHz |  | | c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |  | | d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |  | | e | Interfejsy sieciowe | 2 x 1Gb |  | | f | Moduł zarządzania | Wymagany |  | | g | System operacyjny | CentOS z możliwością upgrade do nowszej wersji lub równoważny |  | | h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |  | | 6 | Serwery (Update) x 1 | Minimalne wymagania Zamawiającego |  | | a | Architektura | x86-64 |  | | b | Pamięć podstawowa | 2 GB DDR3 1333MHz |  | | c | Procesor/Procesory | 2 x 2-core 2,40GHz (E5-2660 V.2) min. 500 punktów w teście PECint\_rate\_2006 |  | | d | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |  | | e | Interfejsy sieciowe | 2 x 1Gb |  | | f | Moduł zarządzania | Wymagany |  | | g | System operacyjny | Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny |  | | h | Przestrzeń dyskowa | 100 GB (5.000 IOPS) |  | |
| 1. SPEŁNIENIE STANDARDÓW ISO 27001, ISO 22301 |
| Wykonawca, **a w przypadku Wykonawców wspólnie ubiegających się o zamówienie każdy** **z nich**, zapewnia że:   1. spełnia standardy ISO 27001 (lub porównywalnego systemu o standardach nie niższych niż wskazana norma), co potwierdza posiadany przez Wykonawcę ważny (aktualny) certyfikat wydany przez niezależny podmiot zajmujący się poświadczaniem zgodności działań z System Zarządzania Bezpieczeństwem Informacji ISO 27001 lub z porównywalnym systemem o standardach nie niższych niż wskazana norma   TAK\* ☐ NIE\* ☐  W przypadku zaznaczenia odpowiedzi „TAK” podać dane identyfikujące certyfikat: ……………………………………………………………………………………………..……………………… *(oznaczenie, nr, jednostka certyfikująca)*   1. spełnia standardy ISO 22301 (lub porównywalnego systemu o standardach nie niższych niż wskazana norma), co potwierdza posiadany przez Wykonawcę ważny (aktualny) certyfikat wydany przez niezależny podmiot zajmujący się poświadczaniem zgodności działań z System Zarządzania Ciągłością Działania ISO 22301 lub z porównywalnym systemem o standardach nie niższych niż wskazana norma   TAK\* ☐ NIE\* ☐  W przypadku zaznaczenia odpowiedzi „TAK” podać dane identyfikujące certyfikat: ……………………………………………………………………………………………..…………… *(oznaczenie, nr, jednostka certyfikująca)*    *\*zaznaczyć właściwe* |

Ponadto oświadczamy, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

Podpisy:

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Miejscowość  i data | Osoby uprawnione do występowania  w obrocie prawnym lub posiadające pełnomocnictwo | |
| Imię i nazwisko | Podpis |
|  |  |  |  |