**Załącznik nr 3a**

**(wzór)**

**PROTOKÓŁ ZDAWCZO – ODBIORCZY**

**do umowy nr …………… z dnia ………………**

Miejscowość: Wrocław data odbioru .....................................

1. **Zamawiający:**

4 Wojskowy Szpital Kliniczny z Polikliniką

Samodzielny Publiczny Zakład Opieki Zdrowotnej

ul. Weigla 5

50-981 Wrocław

w imieniu którego odbioru dokonują:

……………………………………………

imię i nazwisko

……………………………………………

imię i nazwisko

**Wykonawca:**

………………………………………………………………

………………………………………………………………

………………………………………………………………

w imieniu którego sprzęt przekazuje:

…………………………………………… …………………………………...

imię i nazwisko stanowisko

1. Przedmiot protokołu……………………………………………………………………

typ ……………………, rok produkcji …………, producent ……………:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NAZWA | Numer katalogowy /TYP | ILOŚĆ SZTUK | Numer  seryjny | Kod SSM |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Odbiorca potwierdza otrzymanie wraz z dostarczonym sprzętem medycznym :

* instrukcji obsługi i użytkowania w języku polskim w formie papierowej i elektronicznej wykazu autoryzowanych punktów serwisowych,
* Kopii Certyfikatu CE wydanego przez jednostkę notyfikowaną (jeżeli dotyczy) wraz z tłumaczeniem w przypadku oryginału w jęz. obcym,
* Kopii Deklaracji Zgodności wystawioną przez producenta wraz z tłumaczeniem w przypadku oryginału w jęz. obcym,
* wykaz czynności serwisowych, które mogą być wykonywane przez użytkownika samodzielnie nieskutkujące utratą gwarancji,
* karty gwarancyjnej,
* paszportu technicznego,

1. Szkolenie personelu medycznego w zakresie obsługi, konserwacji, mycia i dezynfekcji przedmiotu przekazania przeprowadzono w dniach:  
   …………………… w godz. ……………
2. W szkoleniu tym wzięły udział następujące osoby:

* …………………………………………………………………
* …………………………………………………………………
* …………………………………………………………………
* …………………………………………………………………
* …………………………………………………………………
* …………………………………………………………………
* …………………………………………………………………
* …………………………………………………………………
* …………………………………………………………………
* …………………………………………………………………

Certyfikaty szkolenia zostaną dosłane do 14 dni od daty podpisania protokołu.

1. Niniejszym zgodnie stwierdzamy, ze sprzęt wymieniony w pkt. 2 niniejszego protokołu zostaje przyjęty do eksploatacji **bez zastrzeżeń.**

**Wykonawca: Zamawiający:**

**Załącznik nr 3b**

**Lista pracowników Wykonawcy**

**Wykaz osób uprawnionych przez Wykonawcę do realizacji przedmiotu umowy   
Nr …………..……..; §….. ust….. , spełniających wymogi niniejszej umowy, którym nadano upoważnienia do przetwarzania danych oraz które złożyły oświadczenie o zachowaniu poufności**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Imię i nazwisko** | **Nr telefonu** | **Adres e-mail** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

…………..… dnia…………… ......................................................................

*(podpis i pieczęć Wykonawcy lub osoby upełnomocnionej przez Wykonawcę)*

**Załącznik nr 3c**

**( wzór)**

**ZASADY UDZIELANIA ZDALNEGO DOSTĘPU DO SI**

„WZÓR - LISTA PRACOWNIKÓW - ZASADY UDZIELENIA ZDALNEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO”

Niniejszy załącznik ustala zasady udzielenia Wykonawcy zdalnego dostępu do zasobów sieci teleinformatycznej Zamawiającego w celu umożliwienia Wykonawcy realizacji jego zobowiązań wynikających z umowy, w szczególności określonych w §2:

**§ 1 Udostępnienie**

1. Zdalny Dostęp zostanie udostępniony Wykonawcy przez Zamawiającego w terminie   
   14 dni od daty złożenia wniosku o udostępnienie – po spełnieniu przez Wykonawcę wszystkich wymagań Ośrodka Informatyki 4. WSzKzP SPZOZ we Wrocławiu.
2. Zdalny Dostęp udostępniony zostanie na cały czas trwania niniejszej umowy.
3. Lista osób Wykonawcy uprawnionych do Zdalnego Dostępu:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Imię i nazwisko** | **Nr telefonu** | **Adres e-mail** | **Data ważności uprawnienia** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Bezpośredni dostęp do systemów Zamawiającego jest możliwy tylko i wyłącznie po udostępnieniu go przez administratora Zamawiającego i po przekazaniu wymaganych uprawnień i haseł.
2. W przypadku zgłoszenia błędu krytycznego Zamawiający zapewni sprawne działanie zdalnego dostępu.

**§ 2 Zasady korzystania**

1. Korzystając ze Zdalnego Dostępu Wykonawca:
   1. będzie wykorzystywał Zdalny Dostęp wyłącznie w celu realizacji niniejszej umowy;
   2. nie będzie pozyskiwał ani przetwarzał żadnych innych danych, za wyjątkiem danych niezbędnych do realizacji niniejszej umowy;
2. Zabrania się Wykonawcy przekazywania danych logowania (login lub hasło) innym osobom niż wymienione w § 1 ust. 3 niniejszego załącznika.
3. Zdalny dostęp udostępnia się tylko do przeglądu danych.

**§ 3 Warunki Techniczne do uzyskania Zdalnego Dostępu**

1. Wykonawca dostarczy listę komputerów (wraz z adresami IP), z których będzie realizował Zdalny Dostęp do sieci teleinformatycznej Zamawiającego.
2. Zamawiający zapewni jeden z czterech rodzajów połączeń:
   1. VPN - zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie bezpiecznego kanału VPN;
   2. Udostępnienie terminala - zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie bezpiecznego terminala;
   3. Udostępnienie portu do bazy danych – zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie IP i portu pozwalającego na komunikację z bazą danych.
3. Zamawiający przekaże każdej osobie z podanej listy użytkowników Wykonawcy, określonych   
   w § 1 ust. 3 niniejszego załącznika, zestaw odpowiadających im identyfikatorów użytkowników (login) wraz z ich hasłami dostępu oraz innymi parametrami niezbędnymi do zestawienia zdalnego połączenia. Użytkownicy po stronie Wykonawcy zobowiązują się do nie udostępniania tych identyfikatorów i haseł innym osobom oraz wykorzystywania dostępu wyłącznie w celu realizacji niniejszej Umowy.
4. Wszystkie dane dotyczące parametrów logowania zostaną przekazane na indywidualne konta   
   e-mail. Tą samą drogą dostarczone zostanie również oprogramowanie Klienta VPN lub klienta terminalowego. Oprogramowanie zostanie zainstalowane na komputerach użytkowników staraniem Wykonawcy.

…………..…dnia…………… ..................................................................

*(podpis i pieczęć Wykonawcy lub osoby upełnomocnionej przez Wykonawcę)*

**Załącznik nr 3d**

**WZÓR ZOBOWIĄZANIA DO ZACHOWANIA TAJEMNICY**

Nazwisko ( -ka) : ……………………………....................................................

Imię ( imiona ): 1. .................................................................................

2. ..................................................................................

Dane do kontaktu (podane przez osobę, której dane dotyczą)………………………………………………….

Ja niżej podpisany, potwierdzając zgodność moich danych osobowych ze stanem faktycznym, oświadczam, że :

1. Zapoznałem się z treścią ogólnego 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- zwanego (RODO) i wynikających z niego przepisów prawnych.
2. Zostałem uprzedzony, iż dane osobowe i medyczne przetwarzane w Systemie Informatycznym podlegają ustawowej ochronie prawnej.
3. Zobowiązuję się do nieujawniania – w ramach wykonywania prac związanych z realizacją Umowy zawartej pomiędzy 4 Wojskowym Szpitalem Klinicznym z Polikliniką we Wrocławiu a firmą ………………….. informacji chronionych.
4. Zobowiązuję się do nierozpowszechniania nabytej informacji o charakterze technicznym, technologicznym, organizacyjnym i handlowym, chronionej przez 4 Wojskowy Szpital Kliniczny z Polikliniką we Wrocławiu pod rygorem odpowiedzialności cywilnej i karnej.
5. Obowiązek zachowania w tajemnicy informacji dotyczących wyżej wymienionych danych uzyskanych   
   w związku z realizacją zadań wynikających z przedmiotu Umowy zawartej pomiędzy 4 Wojskowym Szpitalem Klinicznym z Polikliniką we Wrocławiu a firmą ……………….ciąży na mnie nawet po wygaśnięciu stosunku o pracę.

Powyższe zobowiązanie zachowuje ważność w przypadku danych osobowych i medycznych bezterminowo,   
a w przypadku pozostałych danych przez cały okres trwania Umowy.

.................................. dnia ..................... Podpis pracownika : ………………...............................................

*Załącznik Nr 3e*

**WYKAZ ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH,   
KTÓRE ZOBOWIĄZANY JEST WDROŻYĆ PROCESOR**

W celu zapewnienia odpowiedniego stopnia zabezpieczenia powierzonych danych Procesor jest zobowiązany:

1. wdrożyć środki techniczne i organizacyjne:

* zapewniające możliwość ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów służących do przetwarzania danych osobowych oraz usług przetwarzania;
* zapewniające możliwość szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

1. dokonywać regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych;
2. **Proszę odpowiednio zaznaczyć odpowiedź TAK lub NIE.**

|  |  |  |
| --- | --- | --- |
| **Środki organizacyjne** | **TAK** | **NIE** |
| Wdrożona Polityka Bezpieczeństwa Informacji |  |  |
| Wdrożona Polityka Bezpieczeństwa Teleinformatycznego |  |  |
| Wdrożona procedura w zakresie zarządzania uprawnieniami do systemów informatycznych przetwarzających dane osobowe |  |  |
| Wdrożona procedura w zakresie bezpiecznego logowania i zarządzania hasłami |  |  |
| Wdrożona procedura w zakresie zarządzania systemami informatycznymi |  |  |
| Wdrożona procedura w zakresie dostępu do budynków, pomieszczeń i systemów |  |  |
| Wdrożona procedura w zakresie zarządzania bezpieczeństwem urządzeń mobilnych |  |  |
| Wdrożona procedura w zakresie opiniowania oraz akceptacji zmian w projektach oraz infrastrukturze Procesora |  |  |
| Wdrożona procedura w zakresie dostępu do informacji na stacjach roboczych i laptopach z uwzględnieniem zdalnego dostępu użytkowników, administratorów oraz bezpiecznych technologii |  |  |
| Wdrożona procedura w zakresie stosowania certyfikatów oraz zarządzania kluczami |  |  |
| Wdrożona procedura w zakresie ciągłości działania |  |  |
| Stosowanie dobrych praktyk oraz wytycznych w zakresie bezpiecznego tworzenia oprogramowania |  |  |
| Wdrożona Norma ISO…………………………………………………………… |  |  |
| Wyznaczona została osoba pełniąca funkcję IOD nadzorująca przestrzeganie zasad ochrony danych osobowych zgodnie z Ustawą oraz RODO |  |  |
| Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych gwarantująca rozliczalność procesów przetwarzania danych osobowych, zapewnienie poufności, integralności, dostępności przetwarzanych danych osobowych oraz usług przetwarzania |  |  |
| inne regulacje wewnętrzne – uzupełnić jakie……………………..………………………………………………………..  ……………………………………………………………………………………  …………………………………………………………………………………… |  |  |

|  |  |  |
| --- | --- | --- |
| **Środki techniczne** | **TAK** | **NIE** |
| Wdrożona Norma ISO……………………………………………………… |  |  |
| Mechanizmy zapewniające odpowiednie zabezpieczenie przetwarzanych danych osobowych: |  |  |
| * zastosowanie następującej techniki pseudonimizacji ………………………………………………………………………………   ……………………………………………………………………………… |  |  |
| * zastosowanie metody szyfrowania danych osobowych ………………………………………………………………………………   ……………………………………………………………………………….. |  |  |
| * zastosowanie rozwiązania w zakresie ochrony przed złośliwym oprogramowaniem ………………………………………………………………………………   ……………………………………………………………………………… |  |  |
| * zastosowanie zasady bezpiecznego projektowania aplikacji ………………………………………………………………………………   ……………………………………………………………………………….. |  |  |
| * stosowanie rozwiązań i procedur w zakresie bezpiecznego dostępu do informacji na stacjach roboczych i laptopach ze szczególnym uwzględnieniem zdalnego dostępu użytkowników, administratorów oraz bezpiecznych technologii zdalnego dostępu |  |  |
| * stosowanie bezpiecznych rozwiązań w zakresie bezpiecznego uwierzytelniania i autoryzacji oraz bezpiecznego zarządzania hasłami |  |  |
| * stosowanie bezpiecznych mechanizmów w zakresie transmisji danych |  |  |
| * zapewnienie niezbędnych informacji do wyjaśnienia incydentów (np. rejestry logów, informacji z narzędzi monitorujących) |  |  |
| * zapewnienie bezpieczeństwa usług sieciowych ze szczególnym uwzględnieniem usług udostępnianych w sieci publiczne |  |  |

*Załącznik Nr 3f*

**ANKIETA TELETECHNICZNA**

1. Wymagania sprzętowe dla systemu:
   1. serwer:
      1. czy dostawca dostarcza serwer fizyczny
      2. czy dostawca instaluje maszynę wirtualną, korzystając z zasobów szpitala
         1. wymagana liczba procesorów ……………
         2. wymagana ilość pamięci RAM ……………
         3. wymagana ilość miejsca na dysku na serwer (system operacyjny, aplikacje) ………..
         4. wymagana ilość miejsca na dysku na dane …………..
   2. proszę podać nazwę instalowanego na serwerze systemu operacyjnego ……………………………
   3. proszę podać nazwę bazy danych ………………………………………………………………………………………..  
      czy wymagane są dodatkowe licencje, jeśli tak, to czy dostawca je dostarcza …………………….  
      ……………………………………………………………………………………………………………………………………………..
   4. proszę wymienić wszystkie programy, z których korzysta system podczas pracy (pakiet biurowy, podgląd PDF, Java, Flash, itd.) ……………………………………………………………………..……………………………………………………………………..  
      ……………………………………………………………………..……………………………………………………………………..  
      ……………………………………………………………………..……………………………………………………………………..
2. Wymagania sprzętowe dla stacji roboczych (klientów):  
   ……………………………………………………………………………………………………………………………………………..
3. ……………………………………………………………………………………………………………………………………………..
4. ……………………………………………………………………………………………………………………………………………..
5. W jaki sposób realizowana jest archiwizacja danych i backup serwera?  
   ……………………………………………………………………………………………………………………………………………  
   ……………………………………………………………………………………………………………………………………………  
   Jeśli archiwizacja ma być realizowana przez 4WSzKzP, to:
6. - czy dostawca przekaże hasła dostępu dla konta administratora/ root
7. - czy dostawca założy konto przeznaczone do backupów i przekaże hasła dostępu dla konta
8. W przypadku nieprzekazania w/w danych dostępowych, dostawca zobowiązuje się do realizacji archiwizacji danych we własnym zakresie i przekazania harmonogramu archiwizacji podczas wdrożenia.
9. W jaki sposób realizowana jest transmisja danych w ramach systemu:
   1. czy dostarczany system wymaga wpięcia do sieci LAN szpitala …………………………………….  
      ……………………………………………………………………………………………………………………………………..
   2. czy dostarczany system wymaga sieci bezprzewodowej WiFi – kto go realizuje i w jaki sposób   
      ……………………………………………………………………………………………………………………………………..
   3. czy instalowany system wymaga stałego dostępu do internetu,  
      jeśli tak, proszę opisać w jakim celu ………………………………………………………………………………………  
      ……………………………………………………………………………………………………………………………………………..
   4. czy w ramach realizacji umowy jest wymagany dostęp zdalny …………………………………………..
10. Integracja z systemem HIS AMMS

jeśli tak, to proszę opisać sposób integracji:

* 1. czy komunikacja jest zgodna ze standardem HL7
  2. czy wymiana danych obejmuje zlecenia i wyniki
  3. czy dostawca dostarcza licencję na integrację z systemem zewnętrznym wykupioną dla szpitala do systemu AMMS
  4. jeśli system generuje wyniki badań diagnostycznych, to w jaki sposób realizowane są zapisy Rozporządzenia Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania:
     1. czy wyniki badań są podpisywane podpisem elektronicznym?   
        jakim? …………………………………………………………………………
     2. czy wyniki badań są gromadzone w repozytorium EDM?
        1. czy dostawca zapewnia integrację z posiadanym przez szpital repozytorium EDM  
           jeśli tak, to czy dostawca dostarcza licencję na integrację z EDM
        2. czy dostawca zapewnia własne repozytorium?
  5. uwagi …………………………………………………………………………………………………………………………………

…..………………………………………………………………………………………………………………………………………..

1. Integracja z archiwum diagnostyki obrazowej
2. jeśli tak, to proszę opisać sposób integracji:
   1. czy urządzenie posiada kartę sieciową  
       Ethernet  
       WiFi
   2. czy komunikacja jest zgodna ze standardem DICOM 3.0
   3. czy integracja obejmuje wystawianie list roboczych na urządzenia
   4. czy dostawca dostarcza licencję na integrację z systemem zewnętrznym wykupioną dla szpitala do systemu PACS
   5. czy urządzenie wymaga hasła dostępowego do ustawień konfiguracji  
      jeśli tak, to czy dostawca przekaże hasło podczas wdrożenia
   6. uwagi …………………………………………………………………………………………………………………………………

…..………………………………………………………………………………………………………………………………………..