**PAKIET I Załącznik nr 3A**

**DOTYCZY ( NAJEM ) - PROTOKÓŁ INSTALACJI I PRZEKAZANIA**

**do umowy nr …………… z dnia ………………**

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

1. **Zamawiający:**

4. Wojskowy Szpital Kliniczny z Polikliniką

Samodzielny Publiczny Zakład Opieki Zdrowotnej we Wrocławiu

ul. R. Weigla 5

50-981 Wrocław

w imieniu którego odbioru dokonują:

……………………………………………

imię i nazwisko

**Wykonawca:**

………………………………………………………………

………………………………………………………………

………………………………………………………………

w imieniu którego sprzęt przekazuje:

…………………………………………………..…

imię i nazwisko

1. **Przedmiot protokołu** …………………………………………………………… typ ……………………, rok produkcji …………, producent ……………:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NAZWA | 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 notyfikacyjną (jeżeli dotyczy) wraz z tłumaczeniem w przypadku oryginału w jęz. obcym
* kopii Deklaracji Zgodności wystawioną przez producenta wraz z tłumaczeniem w przypadku oryginału w języku obcym
* karty gwarancyjnej
* paszportu technicznego

1. Szkolenie personelu medycznego w zakresie obsługi, konserwacji, mycia i dezynfekcji przedmiotu przekazania przeprowadzono w dniach:  
   …………………… w godz. ……………  
   …………………… 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:**

………..…………………………………

up. pracownik Działu Aparatury

Medycznej

………..…………………………

up. pracownik Oddziału / Zakładu

**PAKIET I Załącznik nr 3B**

**DOTYCZY ( NAJEM ) - PROTOKÓŁ DEINSTALACJI I USUNIĘCIA DANYCH**

**do umowy nr …………… z dnia ………………**

Miejscowość: Wrocław data odbioru …………….

**1. Zamawiający:**

4 Wojskowy Szpital Kliniczny z Polikliniką

Samodzielny Publiczny Zakład Opieki Zdrowotnej we Wrocławiu

ul. R. Weigla 5, 50-981 Wrocław

w imieniu którego przekazania dokonują:

1. Pracownik DAM:

…………………………………………

imię i nazwisko

2. Pracownik Oddziału/Bloku/Pracowni:

…………………………………………

imię i nazwisko

3. Pracownik OI:

…………………………………………

imię i nazwisko

**Wykonawca:**

………………………………………………………………

………………………………………………………………

………………………………………………………………

………………………………………………………………

w imieniu którego sprzęt odbiera:

………………………………………………………………

(imię i nazwisko)

1. **Przedmiot protokołu (dane identyfikacyjne urządzenia/pamięci)** ……………………………………………………………………… typ ……………………, rok produkcji …………, producent ……………:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa sprzętu** | **Typ** | **Ilość sztuk** | **Numer**  **seryjny** | **kod SSM** | **Nazwa programu do kasowania DO** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Opis zastosowanej procedury bezpowrotnego niszczenia DO – każdorazowo pod nadzorem OI** ………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**----------------------------------------------------------------------**

(*data i czytelny podpis osoby dokonującej kasowania DO)*

1. **W przypadku braku możliwości realizacji pkt. 3 – przekazanie na własność dysków Zamawiającemu – zgodnie z zapisami § 4 pkt. 8 niniejszej umowy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *NAZWA* | *Typ* | *ILOŚĆ SZTUK* | *Numer*  *seryjny* | *kod SSM* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Niniejszym zgodnie stwierdzamy, ze sprzęt wymieniony w pkt. 2 niniejszego protokołu zostaje przekazany **bez zastrzeżeń, (wpisać uwagi lub zastrzeżenia)**

**……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….**

**Wykonawca: Zamawiający:**

………..………………..………………………

up. pracownik Działu Aparatury Medycznej

……………………………………………………

up. pracownik Ośrodka Informatyki (jeżeli dotyczy)

………………………..…………………………

up. pracownik Oddziału

**PAKIET I Załącznik nr *3C***

**Wykaz środków organizacyjnych i technicznych, które zobowiązany jest wdrożyć podmiot przetwarzający do umowy nr…. z dnia……**

W celu zapewnienia odpowiedniego stopnia zabezpieczenia powierzonych danych podmiot przetwarzający (PP) jest zobowiązany:

1. **wdrożyć środki techniczne i organizacyjne**:

* zapewniające możliwość ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów służących do przetwarzania danych w tym 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 zaznaczyć stosując znak X odpowiedź TAK lub NIE, ew. poszerzyć odpowiedź .**

|  |  |  |  |
| --- | --- | --- | --- |
| **Środki organizacyjne** | **TAK** | **NIE** | **Odp.** |
| \*Czy PP stosuje zatwierdzony kodeks postępowania? Jeśli TAK to jaki? |  |  |  |
| \*Czy PP posiada certyfikowany System Zarządzania Bezpieczeństwem Informacji .Wdrożenie potwierdzone certyfikatem nr..  Wydany przez…..Ważny do…… |  |  |  |
| \**Jeżeli podmiot przetwarzający stosuje zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji, dodatkowa weryfikacja nie jest wymagana (.preambuła RODO motyw 81)* |  |  |  |
| Czy PP posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? |  |  |  |
| Czy PP jest w stanie wykazać przestrzeganie danych zasad dotyczących przetwarzania danych osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych? |  |  |  |
| Czy PP dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych ? |  |  |  |
| Czy PP zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? |  |  |  |
| Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? |  |  |  |
| Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od PP imienne upoważnienia do przetwarzania danych, czy upoważnienia są cyklicznie weryfikowane? |  |  |  |
| Czy podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania ? |  |  |  |
| Czy PP prowadzi analizę ryzyka dla zasobów biorących udział w operacjach przetwarzania i posiada stosowne raporty z przeprowadzonej analizy ryzyka |  |  |  |
| Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |  |  |
| Czy PP posiada wdrożoną procedurę zgłaszania naruszeń ochrony danych do organu nadzorczego UODO |  |  |  |
| Czy PP posiada procedury odtwarzania systemu po awarii oraz ich testowania |  |  |  |
| Czy PP posiada plan ciągłości działania |  |  |  |
| Czy PP ma wdrożone wymagania normy System Zarządzania Bezpieczeństwem Informacji ISO 27001 |  |  |  |
| 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  Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania? |  |  |  |
| Wdrożona procedura w zakresie zarządzania bezpieczeństwem urządzeń mobilnych:  Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu?  Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne?  Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe? |  |  |  |
| 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 |  |  |  |
| inne regulacje wewnętrzne – proszę uzupełnić |  |  |  |
| **Bezpieczeństwo fizyczne i środowiskowe** |  |  |  |
| Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |  |  |
| Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany? |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Środki techniczne** | **TAK** | | | **NIE** | **Odp.** |
| Mechanizmy zapewniające odpowiednie zabezpieczenie przetwarzanych danych osobowych: |  | | |  |  |
| * zastosowanie następującej techniki pseudonimizacji ………………………………………………………………………………   ……………………………………………………………………………… |  | | |  |  |
| * zastosowanie metody szyfrowania danych osobowych ………………………………………………………………………………   ………………………………………………………………………… |  | | |  |  |
| * zastosowanie rozwiązania w zakresie ochrony przed złośliwym oprogramowaniem ………………………………………………………………………………   ……………………………………………………………………………… |  | | |  |  |
| * zastosowane środki zabezpieczające przed wyciekiem danych……………..   ………………………………………………………………………………….. |  | | |  |  |
| * 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 |  | | |  |  |
| * Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  | | |  |  |
| Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych? |  | |  | |  |
| Gdzie są przechowywane kopie zapasowe? |  | |  | |  |
| Czy organizacja wdraża nowe rozwiązania zgodnie z zasadą "privacy by design"? |  | |  | |  |
| Czy organizacja działa zgodnie z zasadą "privacy by default"? |  |  | | |  |

|  |  |
| --- | --- |
| dnia………………… | (podpis i pieczęć Wykonawcy lub osoby upełnomocnionej przez Wykonawcę) |

**PAKIET I Załącznik nr *3D***

**ANKIETA TELETECHNICZNA**

|  |  |  |
| --- | --- | --- |
| 1) Wymagania sprzętowe dla systemu: | Proszę zaznaczyć odpowiedź stosując  znak X | |
| a) serwer | **TAK** | **NIE** |
| czy dostawca dostarcza serwer fizyczny? |  |  |
| 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 …………..
  1. proszę podać nazwę instalowanego na serwerze systemu operacyjnego …………………………………………………………………………………………
  2. proszę podać nazwę bazy danych …………………………………………………………………………………………  
     czy wymagane są dodatkowe licencje, jeśli tak, to czy dostawca je dostarcza ………  
     …………………………………………………………………………………………
  3. proszę wymienić wszystkie programy, z których korzysta system podczas pracy (pakiet biurowy, podgląd PDF, Java, Flash, itd.) ……………………………………………………………………..………………………………………………………………………………………………………………..

1. Wymagania sprzętowe dla stacji roboczych (klientów):  
   ………………………………………………………………………………………………………………………………………………………………………………………………
2. W jaki sposób realizowana jest archiwizacja danych i backup serwera?  
   ………………………………………………………………………………………………….…………………………………………………………………………………………..

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy archiwizacja ma być realizowana przez 4WSzKzP ? |  |  |
| Czy dostawca przekaże hasła dostępu dla konta administratora/root? |  |  |
| Czy dostawca założy konto przeznaczone do backupów i przekaże hasła dostępu dla konta? |  |  |

W przypadku nieprzekazania w/w danych dostępowych, dostawca zobowiązuje się do realizacji archiwizacji danych we własnym zakresie i przekazania harmonogramu archiwizacji podczas wdrożenia.

1. 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?
2. Integracja z systemem HIS AMMS, jeśli tak, proszę opisać sposób integracji:

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy komunikacja jest zgodna ze standardem HL7 |  |  |
| Czy wymiana danych obejmuje zlecenia i wyniki |  |  |
| Czy dostawca dostarcza licencję na integrację z systemem zewnętrznym wykupioną dla szpitala do systemu AMMS |  |  |

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:

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy wyniki badań są podpisywane podpisem elektronicznym?  jakim? |  |  |
| Czy wyniki badań są gromadzone w repozytorium EDM? |  |  |
| Czy dostawca zapewnia integrację z posiadanym przez szpital repozytorium EDM |  |  |
| jeśli tak, to czy dostawca dostarcza licencję na integrację z EDM |  |  |
| Czy dostawca zapewnia własne repozytorium? |  |  |

Uwagi……………………………………………………………………………………………6) Integracja z archiwum diagnostyki obrazowej, jeśli tak, proszę opisać sposób integracji:

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy urządzenie posiada kartę sieciową? |  |  |
| Ethernet |  |  |
| Wi-Fi |  |  |
| Czy komunikacja jest zgodna ze standardem DICOM 3.0 |  |  |
| Czy integracja obejmuje wystawianie list roboczych na urządzenia |  |  |
| Czy dostawca dostarcza licencję na integrację z systemem zewnętrznym wykupioną dla szpitala do systemu PACS |  |  |
| Czy urządzenie wymaga hasła dostępowego do ustawień konfiguracji |  |  |
| jeśli tak, to czy dostawca przekaże hasło podczas wdrożenia |  |  |

Uwagi………………………………………………………………………………………..

Dnia……………………………………………………………………………………………

(podpis i pieczęć Wykonawcy lub osoby upełnomocnionej przez Wykonawcę)

**PAKIET I Załącznik nr *3E***

**Wykaz osób uprawnionych przez Wykonawcę do realizacji przedmiotu umowy**

**Nr …………..…….. 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)*

**PAKIET I Załącznik nr *3F***

**ZASADY UDZIELANIA ZDALNEGO DOSTĘPU DO WYBRANEGO SI EKSPLOATOWANEGO W 4. WSzKzP SPOZ WE WROCŁAWIU**

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 nadany Wykonawcy przez Zamawiającego w terminie   
   3 dni od daty złożenia wniosku o udostępnienie – po spełnieniu przez Wykonawcę wszystkich wymagań Ośrodka Informatyki 4. WSzKzP SPZOZ we Wrocławiu.
2. Zdalny Dostęp nadany 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 Warunki Techniczne do uzyskania Zdalnego Dostępu**

1. Wykonawca dostarczy listę adresów IP, z których będzie realizował Zdalny Dostęp do sieci teleinformatycznej Zamawiającego.
2. Zamawiający zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie bezpiecznego kanału VPN typu IPSEC.
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 nieudostępniania 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 typu klient VPN. Oprogramowanie zostanie zainstalowane na komputerach użytkowników staraniem Wykonawcy.

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

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

**PAKIET I Załącznik nr *3G***

**ZOBOWIĄZANIE 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 lub umowy cywilnoprawnej.

Powyższe zobowiązanie zachowuje ważność bezterminowo.

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

**PAKIET I Załącznik nr *3H***

**CYBERBEZPIECZEŃSTWO**

1. Oprogramowanie musi realizować wszystkie swoje funkcje przy włączonym oprogramowaniu antywirusowym i przy włączonej zaporze Windows wykorzystywanej przez Zamawiającego, a także przy włączonych mechanizmach bezpieczeństwa wbudowanych w system operacyjny serwera. Niedopuszczalne jest wyłączanie jakiejkolwiek z powyższych funkcji.

2. Oprogramowanie musi dopuszczać tylko niezbędny ruch do prawidłowego funkcjonowania oprogramowania (hardening)

3. Oprogramowanie musi realizować wszystkie swoje funkcje przy włączonym oprogramowaniu realizującym wykrywanie i reagowanie na incydenty cyberbezpieczeństwa w punktach końcowych (EDR)

4. Wykonawca dostarczy pełną dokumentację w zakresie adresów i portów sieciowych, z którymi komunikowało się będzie Oprogramowanie albo będą niezbędne do jego poprawnej pracy.

5. Wykonawca dostarczy pełną specyfikację komunikacji z systemami zewnętrznymi, tj. minimum adresy z którymi ma nastąpić połącznie, nazwy protokołu / numer portu, zakres przesyłanych danych.

6. W przypadku stwierdzenia podatności, zagrożenia bezpieczeństwa cybernetycznego czy incydentu dotyczącego oprogramowania, do którego Wykonawca posiada prawa autorskie, Wykonawca niezwłocznie usunie stwierdzone zdarzenie na własny koszt, zabezpieczając na czas usuwania usterki analogiczne oprogramowanie pozbawione tej podatności. Jeżeli Wykonawca wykorzystuje oprogramowanie firm trzecich jako komponent czy narzędzie systemów własnych, to odpowiedzialność z tytułu podatności na zagrożenia cybernetyczne dotyczy również i tego oprogramowania.

7. Wykonawca zobowiązany jest do wykonywania niezwłocznie po opublikowaniu aktualizacji systemu operacyjnego wraz ze wszystkimi jego komponentami.

8. Oprogramowanie nie może wykorzystywać oprogramowania firm trzecich wobec produktów których stwierdzono występowanie podatności lub wydany został komunikat bezpieczeństwa cybernetycznego o zagrożeniu. W takim przypadku Wykonawca niezwłocznie dokona usunięcia stwierdzonej podatności oprogramowania, ewentualnie zastosuje rozwiązanie zastępcze nieposiadające podatności.

9. Wykonawca wyraża zgodę na instalację na serwerze oprogramowania (typu Agent) posiadanego przez zamawiającego systemu do monitorowania podatności o nazwie Endpoint Central firmy ManageEngine

10. Oprogramowanie monitoruje zdarzenia i zapisuje je w dzienniku zdarzeń (logu).

**PAKIET II Załącznik nr 3A**

**DOTYCZY ( NAJEM ) - PROTOKÓŁ INSTALACJI I PRZEKAZANIA**

**do umowy nr …………… z dnia ………………**

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

1. **Zamawiający:**

4. Wojskowy Szpital Kliniczny z Polikliniką

Samodzielny Publiczny Zakład Opieki Zdrowotnej we Wrocławiu

ul. R. Weigla 5

50-981 Wrocław

w imieniu którego odbioru dokonują:

……………………………………………

imię i nazwisko

**Wykonawca:**

………………………………………………………………

………………………………………………………………

………………………………………………………………

w imieniu którego sprzęt przekazuje:

…………………………………………………..…

imię i nazwisko

1. **Przedmiot protokołu** …………………………………………………………… typ ……………………, rok produkcji …………, producent ……………:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NAZWA | 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 notyfikacyjną (jeżeli dotyczy) wraz z tłumaczeniem w przypadku oryginału w jęz. obcym
* kopii Deklaracji Zgodności wystawioną przez producenta wraz z tłumaczeniem w przypadku oryginału w języku obcym
* karty gwarancyjnej
* paszportu technicznego

1. Szkolenie personelu medycznego w zakresie obsługi, konserwacji, mycia i dezynfekcji przedmiotu przekazania przeprowadzono w dniach:  
   …………………… w godz. ……………  
   …………………… 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:**

………..…………………………………

up. pracownik Działu Aparatury

Medycznej

………..…………………………

up. pracownik Oddziału / Zakładu

**PAKIET II Załącznik nr 3B**

**DOTYCZY ( NAJEM ) - PROTOKÓŁ DEINSTALACJI I USUNIĘCIA DANYCH**

**do umowy nr …………… z dnia ………………**

Miejscowość: Wrocław data odbioru …………….

**1. Zamawiający:**

4 Wojskowy Szpital Kliniczny z Polikliniką

Samodzielny Publiczny Zakład Opieki Zdrowotnej we Wrocławiu

ul. R. Weigla 5, 50-981 Wrocław

w imieniu którego przekazania dokonują:

1. Pracownik DAM:

…………………………………………

imię i nazwisko

2. Pracownik Oddziału/Bloku/Pracowni:

…………………………………………

imię i nazwisko

3. Pracownik OI:

…………………………………………

imię i nazwisko

**Wykonawca:**

………………………………………………………………

………………………………………………………………

………………………………………………………………

………………………………………………………………

w imieniu którego sprzęt odbiera:

………………………………………………………………

(imię i nazwisko)

1. **Przedmiot protokołu (dane identyfikacyjne urządzenia/pamięci)** ……………………………………………………………………… typ ……………………, rok produkcji …………, producent ……………:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa sprzętu** | **Typ** | **Ilość sztuk** | **Numer**  **seryjny** | **kod SSM** | **Nazwa programu do kasowania DO** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Opis zastosowanej procedury bezpowrotnego niszczenia DO – każdorazowo pod nadzorem OI**…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**----------------------------------------------------------------------**

(*data i czytelny podpis osoby dokonującej kasowania DO)*

1. **W przypadku braku możliwości realizacji pkt. 3 – przekazanie na własność dysków Zamawiającemu – zgodnie z zapisami § 4 pkt. 8 niniejszej umowy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *NAZWA* | *Typ* | *ILOŚĆ SZTUK* | *Numer*  *seryjny* | *kod SSM* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Niniejszym zgodnie stwierdzamy, ze sprzęt wymieniony w pkt. 2 niniejszego protokołu zostaje przekazany **bez zastrzeżeń, (wpisać uwagi lub zastrzeżenia)**

**……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….**

**Wykonawca: Zamawiający:**

………..………………..………………………

up. pracownik Działu Aparatury Medycznej

……………………………………………………

up. pracownik Ośrodka Informatyki (jeżeli dotyczy)

………………………..…………………………

up. pracownik Oddziału

**PAKIET III Załącznik nr 3A**

**DOTYCZY ( NAJEM ) - PROTOKÓŁ INSTALACJI I PRZEKAZANIA**

**do umowy nr …………… z dnia ………………**

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

1. **Zamawiający:**

4. Wojskowy Szpital Kliniczny z Polikliniką

Samodzielny Publiczny Zakład Opieki Zdrowotnej we Wrocławiu

ul. R. Weigla 5

50-981 Wrocław

w imieniu którego odbioru dokonują:

……………………………………………

imię i nazwisko

**Wykonawca:**

………………………………………………………………

………………………………………………………………

………………………………………………………………

w imieniu którego sprzęt przekazuje:

…………………………………………………..…

imię i nazwisko

1. **Przedmiot protokołu** …………………………………………………………… typ ……………………, rok produkcji …………, producent ……………:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NAZWA | 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 notyfikacyjną (jeżeli dotyczy) wraz z tłumaczeniem w przypadku oryginału w jęz. obcym
* kopii Deklaracji Zgodności wystawioną przez producenta wraz z tłumaczeniem w przypadku oryginału w języku obcym
* karty gwarancyjnej
* paszportu technicznego

1. Szkolenie personelu medycznego w zakresie obsługi, konserwacji, mycia i dezynfekcji przedmiotu przekazania przeprowadzono w dniach:  
   …………………… w godz. ……………  
   …………………… 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:**

………..…………………………………

up. pracownik Działu Aparatury

Medycznej

………..…………………………

up. pracownik Oddziału / Zakładu

**PAKIET III Załącznik nr 3B**

**DOTYCZY ( NAJEM ) - PROTOKÓŁ DEINSTALACJI I USUNIĘCIA DANYCH**

**do umowy nr …………… z dnia ………………**

Miejscowość: Wrocław data odbioru …………….

**1. Zamawiający:**

4 Wojskowy Szpital Kliniczny z Polikliniką

Samodzielny Publiczny Zakład Opieki Zdrowotnej we Wrocławiu

ul. R. Weigla 5, 50-981 Wrocław

w imieniu którego przekazania dokonują:

1. Pracownik DAM:

…………………………………………

imię i nazwisko

2. Pracownik Oddziału/Bloku/Pracowni:

…………………………………………

imię i nazwisko

3. Pracownik OI:

…………………………………………

imię i nazwisko

**Wykonawca:**

………………………………………………………………

………………………………………………………………

………………………………………………………………

………………………………………………………………

w imieniu którego sprzęt odbiera:

………………………………………………………………

(imię i nazwisko)

1. **Przedmiot protokołu (dane identyfikacyjne urządzenia/pamięci)** ……………………………………………………………………… typ ……………………, rok produkcji …………, producent ……………:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa sprzętu** | **Typ** | **Ilość sztuk** | **Numer**  **seryjny** | **kod SSM** | **Nazwa programu do kasowania DO** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Opis zastosowanej procedury bezpowrotnego niszczenia DO – każdorazowo pod nadzorem OI**…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**----------------------------------------------------------------------**

(*data i czytelny podpis osoby dokonującej kasowania DO)*

1. **W przypadku braku możliwości realizacji pkt. 3 – przekazanie na własność dysków Zamawiającemu – zgodnie z zapisami § 4 pkt. 8 niniejszej umowy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *NAZWA* | *Typ* | *ILOŚĆ SZTUK* | *Numer*  *seryjny* | *kod SSM* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Niniejszym zgodnie stwierdzamy, ze sprzęt wymieniony w pkt. 2 niniejszego protokołu zostaje przekazany **bez zastrzeżeń, (wpisać uwagi lub zastrzeżenia)**

**……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….**

**Wykonawca: Zamawiający:**

………..………………..………………………

up. pracownik Działu Aparatury Medycznej

……………………………………………………

up. pracownik Ośrodka Informatyki (jeżeli dotyczy)

………………………..…………………………

up. pracownik Oddziału

**PAKIET III Załącznik nr *3C***

**Wykaz środków organizacyjnych i technicznych, które zobowiązany jest wdrożyć podmiot przetwarzający do umowy nr…. z dnia……**

W celu zapewnienia odpowiedniego stopnia zabezpieczenia powierzonych danych podmiot przetwarzający (PP) jest zobowiązany:

1. **wdrożyć środki techniczne i organizacyjne**:

* zapewniające możliwość ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów służących do przetwarzania danych w tym 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 zaznaczyć stosując znak X odpowiedź TAK lub NIE, ew. poszerzyć odpowiedź .**

|  |  |  |  |
| --- | --- | --- | --- |
| **Środki organizacyjne** | **TAK** | **NIE** | **Odp.** |
| \*Czy PP stosuje zatwierdzony kodeks postępowania? Jeśli TAK to jaki? |  |  |  |
| \*Czy PP posiada certyfikowany System Zarządzania Bezpieczeństwem Informacji .Wdrożenie potwierdzone certyfikatem nr..  Wydany przez…..Ważny do…… |  |  |  |
| \**Jeżeli podmiot przetwarzający stosuje zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji, dodatkowa weryfikacja nie jest wymagana (.preambuła RODO motyw 81)* |  |  |  |
| Czy PP posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? |  |  |  |
| Czy PP jest w stanie wykazać przestrzeganie danych zasad dotyczących przetwarzania danych osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych? |  |  |  |
| Czy PP dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych ? |  |  |  |
| Czy PP zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? |  |  |  |
| Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? |  |  |  |
| Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od PP imienne upoważnienia do przetwarzania danych, czy upoważnienia są cyklicznie weryfikowane? |  |  |  |
| Czy podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania ? |  |  |  |
| Czy PP prowadzi analizę ryzyka dla zasobów biorących udział w operacjach przetwarzania i posiada stosowne raporty z przeprowadzonej analizy ryzyka |  |  |  |
| Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |  |  |
| Czy PP posiada wdrożoną procedurę zgłaszania naruszeń ochrony danych do organu nadzorczego UODO |  |  |  |
| Czy PP posiada procedury odtwarzania systemu po awarii oraz ich testowania |  |  |  |
| Czy PP posiada plan ciągłości działania |  |  |  |
| Czy PP ma wdrożone wymagania normy System Zarządzania Bezpieczeństwem Informacji ISO 27001 |  |  |  |
| 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  Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania? |  |  |  |
| Wdrożona procedura w zakresie zarządzania bezpieczeństwem urządzeń mobilnych:  Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu?  Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne?  Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe? |  |  |  |
| 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 |  |  |  |
| inne regulacje wewnętrzne – proszę uzupełnić |  |  |  |
| **Bezpieczeństwo fizyczne i środowiskowe** |  |  |  |
| Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |  |  |
| Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany? |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Środki techniczne** | **TAK** | | | **NIE** | **Odp.** |
| Mechanizmy zapewniające odpowiednie zabezpieczenie przetwarzanych danych osobowych: |  | | |  |  |
| * zastosowanie następującej techniki pseudonimizacji ………………………………………………………………………………   ……………………………………………………………………………… |  | | |  |  |
| * zastosowanie metody szyfrowania danych osobowych ………………………………………………………………………………   ………………………………………………………………………… |  | | |  |  |
| * zastosowanie rozwiązania w zakresie ochrony przed złośliwym oprogramowaniem ………………………………………………………………………………   ……………………………………………………………………………… |  | | |  |  |
| * zastosowane środki zabezpieczające przed wyciekiem danych……………..   ………………………………………………………………………………….. |  | | |  |  |
| * 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 |  | | |  |  |
| * Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  | | |  |  |
| Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych? |  | |  | |  |
| Gdzie są przechowywane kopie zapasowe? |  | |  | |  |
| Czy organizacja wdraża nowe rozwiązania zgodnie z zasadą "privacy by design"? |  | |  | |  |
| Czy organizacja działa zgodnie z zasadą "privacy by default"? |  |  | | |  |

|  |  |
| --- | --- |
| dnia………………… | (podpis i pieczęć Wykonawcy lub osoby upełnomocnionej przez Wykonawcę) |

**PAKIET III Załącznik nr *3D***

**ANKIETA TELETECHNICZNA**

|  |  |  |
| --- | --- | --- |
| 1) Wymagania sprzętowe dla systemu: | Proszę zaznaczyć odpowiedź stosując  znak X | |
| a) serwer | **TAK** | **NIE** |
| czy dostawca dostarcza serwer fizyczny? |  |  |
| 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 …………..
  1. proszę podać nazwę instalowanego na serwerze systemu operacyjnego …………………………………………………………………………………………
  2. proszę podać nazwę bazy danych …………………………………………………………………………………………  
     czy wymagane są dodatkowe licencje, jeśli tak, to czy dostawca je dostarcza ………  
     …………………………………………………………………………………………
  3. proszę wymienić wszystkie programy, z których korzysta system podczas pracy (pakiet biurowy, podgląd PDF, Java, Flash, itd.) ……………………………………………………………………..………………………………………………………………………………………………………………..

1. Wymagania sprzętowe dla stacji roboczych (klientów):  
   ………………………………………………………………………………………………………………………………………………………………………………………………
2. W jaki sposób realizowana jest archiwizacja danych i backup serwera?  
   ………………………………………………………………………………………………….…………………………………………………………………………………………..

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy archiwizacja ma być realizowana przez 4WSzKzP ? |  |  |
| Czy dostawca przekaże hasła dostępu dla konta administratora/root? |  |  |
| Czy dostawca założy konto przeznaczone do backupów i przekaże hasła dostępu dla konta? |  |  |

W przypadku nieprzekazania w/w danych dostępowych, dostawca zobowiązuje się do realizacji archiwizacji danych we własnym zakresie i przekazania harmonogramu archiwizacji podczas wdrożenia.

1. 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?
2. Integracja z systemem HIS AMMS, jeśli tak, proszę opisać sposób integracji:

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy komunikacja jest zgodna ze standardem HL7 |  |  |
| Czy wymiana danych obejmuje zlecenia i wyniki |  |  |
| Czy dostawca dostarcza licencję na integrację z systemem zewnętrznym wykupioną dla szpitala do systemu AMMS |  |  |

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:

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy wyniki badań są podpisywane podpisem elektronicznym?  jakim? |  |  |
| Czy wyniki badań są gromadzone w repozytorium EDM? |  |  |
| Czy dostawca zapewnia integrację z posiadanym przez szpital repozytorium EDM |  |  |
| jeśli tak, to czy dostawca dostarcza licencję na integrację z EDM |  |  |
| Czy dostawca zapewnia własne repozytorium? |  |  |

Uwagi……………………………………………………………………………………………6) Integracja z archiwum diagnostyki obrazowej, jeśli tak, proszę opisać sposób integracji:

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy urządzenie posiada kartę sieciową? |  |  |
| Ethernet |  |  |
| Wi-Fi |  |  |
| Czy komunikacja jest zgodna ze standardem DICOM 3.0 |  |  |
| Czy integracja obejmuje wystawianie list roboczych na urządzenia |  |  |
| Czy dostawca dostarcza licencję na integrację z systemem zewnętrznym wykupioną dla szpitala do systemu PACS |  |  |
| Czy urządzenie wymaga hasła dostępowego do ustawień konfiguracji |  |  |
| jeśli tak, to czy dostawca przekaże hasło podczas wdrożenia |  |  |

Uwagi………………………………………………………………………………………..

Dnia……………………………………………………………………………………………

(podpis i pieczęć Wykonawcy lub osoby upełnomocnionej przez Wykonawcę)

**PAKIET III Załącznik nr *3E***

**Wykaz osób uprawnionych przez Wykonawcę do realizacji przedmiotu umowy**

**Nr …………..…….. 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)*

**PAKIET III Załącznik nr *3F***

**ZASADY UDZIELANIA ZDALNEGO DOSTĘPU DO WYBRANEGO SI EKSPLOATOWANEGO W 4. WSzKzP SPOZ WE WROCŁAWIU**

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 nadany Wykonawcy przez Zamawiającego w terminie   
   3 dni od daty złożenia wniosku o udostępnienie – po spełnieniu przez Wykonawcę wszystkich wymagań Ośrodka Informatyki 4. WSzKzP SPZOZ we Wrocławiu.
2. Zdalny Dostęp nadany 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 Warunki Techniczne do uzyskania Zdalnego Dostępu**

1. Wykonawca dostarczy listę adresów IP, z których będzie realizował Zdalny Dostęp do sieci teleinformatycznej Zamawiającego.
2. Zamawiający zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie bezpiecznego kanału VPN typu IPSEC.
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 nieudostępniania 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 typu klient VPN. Oprogramowanie zostanie zainstalowane na komputerach użytkowników staraniem Wykonawcy.

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

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

**PAKIET III Załącznik nr *3G***

**ZOBOWIĄZANIE 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 lub umowy cywilnoprawnej.

Powyższe zobowiązanie zachowuje ważność bezterminowo.

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

**PAKIET III Załącznik nr *3H***

**CYBERBEZPIECZEŃSTWO**

1. Oprogramowanie musi realizować wszystkie swoje funkcje przy włączonym oprogramowaniu antywirusowym i przy włączonej zaporze Windows wykorzystywanej przez Zamawiającego, a także przy włączonych mechanizmach bezpieczeństwa wbudowanych w system operacyjny serwera. Niedopuszczalne jest wyłączanie jakiejkolwiek z powyższych funkcji.

2. Oprogramowanie musi dopuszczać tylko niezbędny ruch do prawidłowego funkcjonowania oprogramowania (hardening)

3. Oprogramowanie musi realizować wszystkie swoje funkcje przy włączonym oprogramowaniu realizującym wykrywanie i reagowanie na incydenty cyberbezpieczeństwa w punktach końcowych (EDR)

4. Wykonawca dostarczy pełną dokumentację w zakresie adresów i portów sieciowych, z którymi komunikowało się będzie Oprogramowanie albo będą niezbędne do jego poprawnej pracy.

5. Wykonawca dostarczy pełną specyfikację komunikacji z systemami zewnętrznymi, tj. minimum adresy z którymi ma nastąpić połącznie, nazwy protokołu / numer portu, zakres przesyłanych danych.

6. W przypadku stwierdzenia podatności, zagrożenia bezpieczeństwa cybernetycznego czy incydentu dotyczącego oprogramowania, do którego Wykonawca posiada prawa autorskie, Wykonawca niezwłocznie usunie stwierdzone zdarzenie na własny koszt, zabezpieczając na czas usuwania usterki analogiczne oprogramowanie pozbawione tej podatności. Jeżeli Wykonawca wykorzystuje oprogramowanie firm trzecich jako komponent czy narzędzie systemów własnych, to odpowiedzialność z tytułu podatności na zagrożenia cybernetyczne dotyczy również i tego oprogramowania.

7. Wykonawca zobowiązany jest do wykonywania niezwłocznie po opublikowaniu aktualizacji systemu operacyjnego wraz ze wszystkimi jego komponentami.

8. Oprogramowanie nie może wykorzystywać oprogramowania firm trzecich wobec produktów których stwierdzono występowanie podatności lub wydany został komunikat bezpieczeństwa cybernetycznego o zagrożeniu. W takim przypadku Wykonawca niezwłocznie dokona usunięcia stwierdzonej podatności oprogramowania, ewentualnie zastosuje rozwiązanie zastępcze nieposiadające podatności.

9. Wykonawca wyraża zgodę na instalację na serwerze oprogramowania (typu Agent) posiadanego przez zamawiającego systemu do monitorowania podatności o nazwie Endpoint Central firmy ManageEngine

10. Oprogramowanie monitoruje zdarzenia i zapisuje je w dzienniku zdarzeń (logu).

**PAKIET IV Załącznik nr 3A**

**DOTYCZY ( NAJEM ) - PROTOKÓŁ INSTALACJI I PRZEKAZANIA**

**do umowy nr …………… z dnia ………………**

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

1. **Zamawiający:**

4. Wojskowy Szpital Kliniczny z Polikliniką

Samodzielny Publiczny Zakład Opieki Zdrowotnej we Wrocławiu

ul. R. Weigla 5

50-981 Wrocław

w imieniu którego odbioru dokonują:

……………………………………………

imię i nazwisko

**Wykonawca:**

………………………………………………………………

………………………………………………………………

………………………………………………………………

w imieniu którego sprzęt przekazuje:

…………………………………………………..…

imię i nazwisko

1. **Przedmiot protokołu** …………………………………………………………… typ ……………………, rok produkcji …………, producent ……………:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NAZWA | 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 notyfikacyjną (jeżeli dotyczy) wraz z tłumaczeniem w przypadku oryginału w jęz. obcym
* kopii Deklaracji Zgodności wystawioną przez producenta wraz z tłumaczeniem w przypadku oryginału w języku obcym
* karty gwarancyjnej
* paszportu technicznego

1. Szkolenie personelu medycznego w zakresie obsługi, konserwacji, mycia i dezynfekcji przedmiotu przekazania przeprowadzono w dniach:  
   …………………… w godz. ……………  
   …………………… 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:**

………..…………………………………

up. pracownik Działu Aparatury

Medycznej

………..…………………………

up. pracownik Oddziału / Zakładu

**Załącznik nr 3B**

**DOTYCZY ( NAJEM ) - PROTOKÓŁ DEINSTALACJI I USUNIĘCIA DANYCH**

**do umowy nr …………… z dnia ………………**

Miejscowość: Wrocław data odbioru …………….

**1. Zamawiający:**

4 Wojskowy Szpital Kliniczny z Polikliniką

Samodzielny Publiczny Zakład Opieki Zdrowotnej we Wrocławiu

ul. R. Weigla 5, 50-981 Wrocław

w imieniu którego przekazania dokonują:

1. Pracownik DAM:

…………………………………………

imię i nazwisko

2. Pracownik Oddziału/Bloku/Pracowni:

…………………………………………

imię i nazwisko

3. Pracownik OI:

…………………………………………

imię i nazwisko

**Wykonawca:**

………………………………………………………………

………………………………………………………………

………………………………………………………………

………………………………………………………………

w imieniu którego sprzęt odbiera:

………………………………………………………………

(imię i nazwisko)

1. **Przedmiot protokołu (dane identyfikacyjne urządzenia/pamięci)** ……………………………………………………………………… typ ……………………, rok produkcji …………, producent ……………:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa sprzętu** | **Typ** | **Ilość sztuk** | **Numer**  **seryjny** | **kod SSM** | **Nazwa programu do kasowania DO** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Opis zastosowanej procedury bezpowrotnego niszczenia DO – każdorazowo pod nadzorem OI**…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**----------------------------------------------------------------------**

(*data i czytelny podpis osoby dokonującej kasowania DO)*

1. **W przypadku braku możliwości realizacji pkt. 3 – przekazanie na własność dysków Zamawiającemu – zgodnie z zapisami § 4 pkt. 8 niniejszej umowy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *NAZWA* | *Typ* | *ILOŚĆ SZTUK* | *Numer*  *seryjny* | *kod SSM* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Niniejszym zgodnie stwierdzamy, ze sprzęt wymieniony w pkt. 2 niniejszego protokołu zostaje przekazany **bez zastrzeżeń, (wpisać uwagi lub zastrzeżenia)**

**……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….**

**Wykonawca: Zamawiający:**

………..………………..………………………

up. pracownik Działu Aparatury Medycznej

……………………………………………………

up. pracownik Ośrodka Informatyki (jeżeli dotyczy)

………………………..…………………………

up. pracownik Oddziału

**Załącznik nr *3C***

**Wykaz środków organizacyjnych i technicznych, które zobowiązany jest wdrożyć podmiot przetwarzający do umowy nr…. z dnia……**

W celu zapewnienia odpowiedniego stopnia zabezpieczenia powierzonych danych podmiot przetwarzający (PP) jest zobowiązany:

1. **wdrożyć środki techniczne i organizacyjne**:

* zapewniające możliwość ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów służących do przetwarzania danych w tym 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 zaznaczyć stosując znak X odpowiedź TAK lub NIE, ew. poszerzyć odpowiedź .**

|  |  |  |  |
| --- | --- | --- | --- |
| **Środki organizacyjne** | **TAK** | **NIE** | **Odp.** |
| \*Czy PP stosuje zatwierdzony kodeks postępowania? Jeśli TAK to jaki? |  |  |  |
| \*Czy PP posiada certyfikowany System Zarządzania Bezpieczeństwem Informacji .Wdrożenie potwierdzone certyfikatem nr..  Wydany przez…..Ważny do…… |  |  |  |
| \**Jeżeli podmiot przetwarzający stosuje zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji, dodatkowa weryfikacja nie jest wymagana (.preambuła RODO motyw 81)* |  |  |  |
| Czy PP posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? |  |  |  |
| Czy PP jest w stanie wykazać przestrzeganie danych zasad dotyczących przetwarzania danych osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych? |  |  |  |
| Czy PP dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych ? |  |  |  |
| Czy PP zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? |  |  |  |
| Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? |  |  |  |
| Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od PP imienne upoważnienia do przetwarzania danych, czy upoważnienia są cyklicznie weryfikowane? |  |  |  |
| Czy podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania ? |  |  |  |
| Czy PP prowadzi analizę ryzyka dla zasobów biorących udział w operacjach przetwarzania i posiada stosowne raporty z przeprowadzonej analizy ryzyka |  |  |  |
| Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |  |  |
| Czy PP posiada wdrożoną procedurę zgłaszania naruszeń ochrony danych do organu nadzorczego UODO |  |  |  |
| Czy PP posiada procedury odtwarzania systemu po awarii oraz ich testowania |  |  |  |
| Czy PP posiada plan ciągłości działania |  |  |  |
| Czy PP ma wdrożone wymagania normy System Zarządzania Bezpieczeństwem Informacji ISO 27001 |  |  |  |
| 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  Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania? |  |  |  |
| Wdrożona procedura w zakresie zarządzania bezpieczeństwem urządzeń mobilnych:  Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu?  Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne?  Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe? |  |  |  |
| 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 |  |  |  |
| inne regulacje wewnętrzne – proszę uzupełnić |  |  |  |
| **Bezpieczeństwo fizyczne i środowiskowe** |  |  |  |
| Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |  |  |
| Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany? |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Środki techniczne** | **TAK** | | | **NIE** | **Odp.** |
| Mechanizmy zapewniające odpowiednie zabezpieczenie przetwarzanych danych osobowych: |  | | |  |  |
| * zastosowanie następującej techniki pseudonimizacji ………………………………………………………………………………   ……………………………………………………………………………… |  | | |  |  |
| * zastosowanie metody szyfrowania danych osobowych ………………………………………………………………………………   ………………………………………………………………………… |  | | |  |  |
| * zastosowanie rozwiązania w zakresie ochrony przed złośliwym oprogramowaniem ………………………………………………………………………………   ……………………………………………………………………………… |  | | |  |  |
| * zastosowane środki zabezpieczające przed wyciekiem danych……………..   ………………………………………………………………………………….. |  | | |  |  |
| * 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 |  | | |  |  |
| * Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  | | |  |  |
| Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych? |  | |  | |  |
| Gdzie są przechowywane kopie zapasowe? |  | |  | |  |
| Czy organizacja wdraża nowe rozwiązania zgodnie z zasadą "privacy by design"? |  | |  | |  |
| Czy organizacja działa zgodnie z zasadą "privacy by default"? |  |  | | |  |

|  |  |
| --- | --- |
| dnia………………… | (podpis i pieczęć Wykonawcy lub osoby upełnomocnionej przez Wykonawcę) |

**ANKIETA TELETECHNICZNA**

**Załącznik nr *3D***

|  |  |  |
| --- | --- | --- |
| 1) Wymagania sprzętowe dla systemu: | Proszę zaznaczyć odpowiedź stosując  znak X | |
| a) serwer | **TAK** | **NIE** |
| czy dostawca dostarcza serwer fizyczny? |  |  |
| 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 …………..
  1. proszę podać nazwę instalowanego na serwerze systemu operacyjnego …………………………………………………………………………………………
  2. proszę podać nazwę bazy danych …………………………………………………………………………………………  
     czy wymagane są dodatkowe licencje, jeśli tak, to czy dostawca je dostarcza ………  
     …………………………………………………………………………………………
  3. proszę wymienić wszystkie programy, z których korzysta system podczas pracy (pakiet biurowy, podgląd PDF, Java, Flash, itd.) ……………………………………………………………………..………………………………………………………………………………………………………………..

1. Wymagania sprzętowe dla stacji roboczych (klientów):  
   ………………………………………………………………………………………………………………………………………………………………………………………………
2. W jaki sposób realizowana jest archiwizacja danych i backup serwera?  
   ………………………………………………………………………………………………….…………………………………………………………………………………………..

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy archiwizacja ma być realizowana przez 4WSzKzP ? |  |  |
| Czy dostawca przekaże hasła dostępu dla konta administratora/root? |  |  |
| Czy dostawca założy konto przeznaczone do backupów i przekaże hasła dostępu dla konta? |  |  |

W przypadku nieprzekazania w/w danych dostępowych, dostawca zobowiązuje się do realizacji archiwizacji danych we własnym zakresie i przekazania harmonogramu archiwizacji podczas wdrożenia.

1. 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?
2. Integracja z systemem HIS AMMS, jeśli tak, proszę opisać sposób integracji:

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy komunikacja jest zgodna ze standardem HL7 |  |  |
| Czy wymiana danych obejmuje zlecenia i wyniki |  |  |
| Czy dostawca dostarcza licencję na integrację z systemem zewnętrznym wykupioną dla szpitala do systemu AMMS |  |  |

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:

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy wyniki badań są podpisywane podpisem elektronicznym?  jakim? |  |  |
| Czy wyniki badań są gromadzone w repozytorium EDM? |  |  |
| Czy dostawca zapewnia integrację z posiadanym przez szpital repozytorium EDM |  |  |
| jeśli tak, to czy dostawca dostarcza licencję na integrację z EDM |  |  |
| Czy dostawca zapewnia własne repozytorium? |  |  |

Uwagi……………………………………………………………………………………………6) Integracja z archiwum diagnostyki obrazowej, jeśli tak, proszę opisać sposób integracji:

|  |  |  |
| --- | --- | --- |
|  | **TAK** | **NIE** |
| Czy urządzenie posiada kartę sieciową? |  |  |
| Ethernet |  |  |
| Wi-Fi |  |  |
| Czy komunikacja jest zgodna ze standardem DICOM 3.0 |  |  |
| Czy integracja obejmuje wystawianie list roboczych na urządzenia |  |  |
| Czy dostawca dostarcza licencję na integrację z systemem zewnętrznym wykupioną dla szpitala do systemu PACS |  |  |
| Czy urządzenie wymaga hasła dostępowego do ustawień konfiguracji |  |  |
| jeśli tak, to czy dostawca przekaże hasło podczas wdrożenia |  |  |

Uwagi………………………………………………………………………………………..

Dnia……………………………………………………………………………………………

(podpis i pieczęć Wykonawcy lub osoby upełnomocnionej przez Wykonawcę)

**Załącznik nr *3E***

**Wykaz osób uprawnionych przez Wykonawcę do realizacji przedmiotu umowy**

**Nr …………..…….. 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 *3F***

**ZOBOWIĄZANIE 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 lub umowy cywilnoprawnej.

Powyższe zobowiązanie zachowuje ważność bezterminowo.

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