Bezpieczeństwo informacji-Wykonawca

(Urządzenie medyczne: Dostawa – **Wykonawca,** wdrożenie, obsługa techniczna i serwisowanie urządzeń/systemów – **Wykonawca)** Załącznik nr 4do Umowy nr 14/AP/2024 (serwis RTG 2197)

l.p	
	Infrastruktura Zamawiającego objęta usługą określoną w umowie (urządzenia/systemy)
1	Wykonawca zapewnia, że jego systemy i aplikacje informatyczne, wszystkie urządzenia (w tym urządzenia komputerowe) stanowiące integralną część serwisowanych urządzeń/systemów objętych umową, na których przetwarzane są dane osobowe są zabezpieczone przed dostępem osób nieupoważnionych oraz przed działaniem szkodliwego oprogramowania o ile producent tych urządzeń tego nie zabrania i jest to technicznie możliwe. Wykonawca zobowiązuje się zabezpieczyć przetwarzane w urządzeniu dane oraz konfigurację tych urządzenia przed utratą danych, nieuprawnioną modyfikacją oraz ich ujawnieniem osobom nieupoważnionym.
2	Wykonawca zapewnia, że do dostęp do urządzeń/systemów informatycznych objętych usługą określoną umową będzie spełniał wymagania nie niższe niż wymagania określone dla infrastruktury Wykonawcy (ze szczególnym uwzględnieniem kont administratorskich na serwisowanych urządzeniach/systemach) o ile jest to możliwe techniczne a producent urządzeń tego nie zabrania.
3	W przypadku dokonywania istotnych zmian w urządzeniach/systemach (np. zmiana konfiguracji) mogących powodować powstanie błędów lub utratę danych osobowych przetwarzanych w urządzeniu, Wykonawca zobowiązany jest do zapewnienia kopii bezpieczeństwa przed podjęciem takich czynności lub uzyskać potwierdzenie Zamawiającego o poprawności przesłania danych z urządzenia do systemu dziedzinowego Zamawiającego (dotyczy urządzeń medycznych).
	Porty komunikacyjne urządzeń objętych usługą określoną w umowie
4	Wykonawca zobowiązuje się do zablokowania portów komunikacyjnych Urządzenia. Odblokowanie portów jest możliwe na pisemne polecenie Zamawiającego lub ich odblokowanie w porozumieniu z Zamawiającym jeśli jest to niezbędne do poprawnego funkcjonowania Urządzenia. Konfiguracja portów przed uruchomieniem produkcyjnym lub dokonaniem zmiany wymaga zatwierdzenia przez co najmniej dwóch uprawnionych i posiadających kwalifikacje serwisantów. Czynności te sa dokumentowane a następnie przekazywane przed odblokowania portów do Zamawiającego.
	Wykonawca i jego infrastruktura wykorzystywana do świadczenia usługi
5	Wykonawca zapewnia, że spełnia wymagania określone u umowie powierzenia przetwarzania w szczególności wymagania, o których mowa w art. 28, 29, 30, 32 RODO.
6	Wykonawca przekaże Zamawiającemu listę serwisantów wykonujących czynności serwisowe urządzeń i systemów objętych Umową oraz dostarczy podpisane przez te osoby oświadczenia o zachowaniu poufności stanowiące **Załącznik nr 5** do Umowy.
7	Wykonawca prowadzi rejestr zasobów informatycznych , które są wykorzystywane do świadczenia usługi (sprzęt, oprogramowanie, sieć) oraz monitoruje ich wykorzystanie. Dla tych zasobów Wykonawca oszacował ryzyko w kontekście bezpieczeństwa informacji oraz zastosował adekwatne zabezpieczenia techniczne i organizacyjne mające minimalizować ryzyko, w szczególności stosuje zabezpieczenia opisane poniżej.
8	Wykonawca zdrożył system zarządzania systemem kontroli dostępu, który umożliwia przydzielanie, modyfikację oraz usuwanie uprawnienia dostępu dla poszczególnych pracowników Wykonawcy do infrastruktury, w której odbywa się przetwarzanie danych osobowych (pomieszczenia, urządzenia, oprogramowanie, sieć), lub z której możliwy jest dostęp do zasobów Zamawiającego przetwarzającej w tym: - stosuje unikatowe nazwa użytkowników oraz złożone hasła uwierzytelniające kont użytkowników do infrastruktury przetwarzającej dane osobowe , - dostęp do powierzonych danych osobowych przetwarzanych w serwisowanych urządzeniach/systemach oraz infrastrukturze Wykonawcy objętych umową będą miały jedynie osoby posiadające uprawnienia do serwisowania tych urządzeń oraz posiadające upoważnienia do przetwarzania danych osobowych. Wykonawca posiada w tym zakresie stosowne procedury i jest w stanie wykazać ich stosowanie, - wykorzystywane urządzenia i systemy mobilne są zarejestrowane i przed dopuszczeniem do wykorzystania są autoryzowane, podlegają kontroli dostępu na takim samym poziomie jak pozostałe urządzenia, i zapewnia, że infrastruktura informatyczna (urządzenia, oprogramowanie, transmisja danych w sieci) jest zabezpieczona przed dostępem osób nieupoważnionych

	oraz przed działaniem szkodliwego oprogramowania. Zarządzanie uprawnieniami jest sformalizowane i udokumentowane.
9	Wykonawca wdrożył, stosuje i aktualizuje procedury i polityki dotyczące bezpieczeństwa informacji (w tym ochrony powierzonych danych osobowych) i jest w stanie je wykazać na żądanie Zamawiającego.
10	Wykonawca zapewnia, że hasła dostępowe do urządzeń/systemów są przechowywane w postaci szyfrowanej.
11	Wszystkie urządzenia mobilne wykorzystywane do świadczenia usługi określonej w umowie są przed dopuszczeniem podlegają szyfrowaniu.
12	W ramach zapewnienia bezpieczeństwa systemów/aplikacji Wykonawca oświadcza, że: - dokłada wszelkich starań aby serwisowane systemy/aplikacje były odpowiednio zabezpieczone i funkcjonowały w sposób uniemożliwiający wyciek danych oraz dostęp osób nieuprawnionych; - Wykonawca ma obowiązek usuwania wykrytych luk i podatności bezpieczeństwa, - ma obowiązek informowania Zamawiającego o wykrytych lukach w zabezpieczeniach i podatnościach urządzeń/systemów objętych umową główną, które mogą zakłócić ciągłość działania Zamawiającego lub mogą mieć wpływ na integralność, poufność i dostępność przetwarzanych danych oraz przedstawić rekomendacje, które zminimalizują ich negatywne skutki do czasu ich usunięcia
	Podwykonawcy Wykonawcy
13	Przed umożliwieniem Podwykonawcy dostępu do powierzonych danych Wykonawca zobowiązany jest uzyskać zatwierdzenie zgłoszonego Podwykonawcy z zastrzeżeniem formy pisemnej (Załącznik do umowy powierzenia przetwarzania danych).
14	Wykonawca oświadcza, że jego Podwykonawcy (mający dostęp do infrastruktury Zamawiającego lub powierzonych danych osobowych) stosują poziom ochrony nie niższy niż określony przez Zamawiającego oraz że ponosi odpowiedzialność za działania Podwykonawców jak za działania własne.
	Konta uprzywilejowane
15	Wykonawca zobowiązuje się do wdrożenia właściwej polityki haseł oraz zarządzenie hasłami uprzywilejowanymi (administratorskie) w celu uniemożliwienia zmian konfiguracyjnych Urządzenia.
	Ochrona podsieci
16	Wykonawca zobowiązany jest do zapewnienia należytego poziomu bezpieczeństwa wydzielonej sieci teleinformatycznej Zamawiającego, w której podłączone są serwisowane Urządzenia m.in. poprzez zastosowania urządzeń/oprogramowania filtrujących ruch do tej sieci (np. firewall).
17	Dla uruchomienie transmisji danych z urządzenia innym medium niż sieć kablowa Ethernet LAN (np. WI-FI , bluetooth lub GSM) wymagana jest pisemna zgoda Zamawiającego. W przypadku planowania uruchomienia takiej transmisji Wykonawca zobowiązany jest do przedstawienia do akceptacji Zamawiającemu oceny skutków dla ochrony danych przesyłanych w taki sposób.
	Nośniki danych i kopie danych
18	Wykonawca oświadcza, że: - w przypadku konieczności wymiany nośników danych (np. dyski HDD,SSD) Urządzeń objętych umową, demontowane z tych urządzeń nośniki zostaną przekazane Zamawiającemu nieodpłatnie, co zostanie potwierdzone stosownym protokołem, - w przypadku konieczności naprawy urządzenia poza terenem Zamawiającego, Wykonawca zdemontuje te nośniki i przekaże je Zamawiającemu przed zabraniem urządzenia do serwisu.
19	Wykonawca zapewnia, że nie będzie wykonywał na zasobach nie należących do Zamawiającego kopii powierzonych do przetwarzania danych osobowych bez pisemnego uprzednio wydanej pisemnej zgody Zamawiającego odrębnej dla każdej planowanej kopii danych. Wykonawca zapewnia, że kopia danych zostanie skutecznie tzn. w sposób nieodwracalny usunięta z zasobów Wykonawcy po zakończeniu czynności serwisowej, dla której wykonanie kopii danych było niezbędne. Z każdego zestawu takich czynności Wykonawca zobowiązany jest niezwłocznie po zakończeniu czynności serwisowej przesłać raport zawierający: zakres skopiowanych danych, określenie czynności serwisowych i niezbędność wykonania kopii, datę i zakres danych podlegających skopiowaniu, określenie rodzaju zasobu, na którym

	została wykonana kopia, datę i potwierdzenie nieodwracalnego usunięcia danych (wraz metodyką usunięcia danych).
20	Przed uruchomieniem produkcyjnym (zasileniem systemu informatycznego danymi osobowymi i podłączenie do infrastruktury Zamawiającego) Wykonawca zobowiązany jest przedstawić Zamawiającemu do akceptacji konfigurację systemu, serwerów i komputerów oraz stosowane zabezpieczenia. Wykonawca ma obowiązek weryfikacji zastosowanej konfiguracji i zabezpieczeń przez dwie niezależne osoby (pracownicy Wykonawcy) . Zasileniem systemu oraz uruchomienie integracji z systemami dziedzinowymi może nastąpić po uzyskaniu od Zamawiającego zatwierdzenia konfiguracji systemów i urządzeń . Zamawiający w porozumieniu z Wykonawcą może przeprowadzić testy penetracyjne wdrażanego systemu przed zasileniem systemu danymi osobowymi.
	Zdalny serwis
21	W sytuacji gdy Zamawiający dopuszcza usługę zdalnego serwisu realizowanej za pośrednictwem sieci publicznej Internet, Wykonawca zapewnia, że podczas zdalnego serwisu urządzeń i systemów objętych Umową komunikacja (przesyłanie danych) pomiędzy tymi systemem teleinformatycznym Zamawiającego a systemem teleinformatycznym Wykonawcy odbywa się w sposób bezpieczny i jest szyfrowana.
22	Przydzielenie zdalnego dostępu dla Wykonawcy będzie się odbywało zgodnie z zasadami obowiązującymi u Zamawiającego (indywidualne konta VPN dla serwisantów). Wykonawca przekaże z zachowaniem formy pisemnej wykaz osób uprawnionych do zestawienia połączenia zdalnego pomiędzy systemami teleinformatycznymi Zamawiającego, a systemem teleinformatycznym Wykonawcy. Sposób realizacji połączenia będzie uzgodniony z Działem Informatyki Zamawiającego.
23	Wykonawca zapewnia, że nie będzie eksportował powierzonych do przetwarzania danych do Państw trzecich (poza obszar EOG). Zapewnia również, że połączenia zdalne do serwisowanych systemów i urządzeń nie będą realizowane z terytorium państwa trzeciego oraz, że nie umożliwi transmisji danych osobowych do państwa trzeciego, które nie zapewnia należytego poziomu ochrony takiego samego jak państwa członkowskie UE (obszar EOG).
24	W związku z realizacją Umowy Wykonawcy zabrania się: a) zmiany przyznanych adresów IP bez uprzedniego uzgodnienia z Zamawiającym, b) rozdzielania sygnału na inne urządzenia niż określony w umowie (np. stosowanie routera itp.), c) jakichkolwiek samowolnych zmian w infrastrukturze telekomunikacyjnej Zamawiającego, d) dokonywania przeciążenia sieci teleinformatycznej Zamawiającego, e) rozsyłania niechcianej poczty (SPAM), f) używania niedozwolonych narzędzi sieciowych, takich jak sniffery, skanery portów, exploity, g) wykorzystywania infrastruktury teleinformatycznej Zamawiającego w celu uruchamiania serwisów świadczących usługi komercyjne, h) rozpowszechniania informacji sprzecznych z obowiązującym prawem oraz naruszających w jakikolwiek sposób uczucia religijne lub normy społeczne i obyczajowe, i) świadczenia usług telekomunikacyjnych osobom trzecim, o ile wiążą się one z tranzytem informacji przez infrastrukturę Zamawiającego, j) prowadzenia jakichkolwiek działań, które mogą powodować zakłócenia w działaniu infrastruktury Zamawiającego, k) podejmowania jakichkolwiek działań, które mogą uszkodzić infrastrukturę Zamawiającego, za pomocą której świadczona jest usługa lub mogących zakłócić poprawne funkcjonowanie systemów służących udostępnianiu i monitorowaniu usługi oraz urządzeń i łączy przeznaczonych do przekazywania informacji na odległość, za pomocą których świadczona jest Usługa, l) dokonywania nieuzgodnionych z Zamawiającym napraw i zmian (w tym również instalacji oprogramowania i urządzeń sieciowych) w infrastrukturze telekomunikacyjnej Zamawiającego, m) stosowania urządzeń sieciowych i oprogramowania nieuzgodnionych z Zamawiającym, n) kierować do infrastruktury Zamawiającego ruchu telekomunikacyjnego z innych sieci telekomunikacyjnych, o) odmowy dostępu do infrastruktury Zamawiającego, w celu przeprowadzenia czynności kontrolnych, konserwacji lub naprawy, p) wykorzystywania udostępnionej przez Zamawiającego infrastruktury niezgodnie z przepisami prawa lub niezgodnie z zawartą Umową, q) uzyskiwania lub podejmowania prób uzyskania informacji z sieci teleinformatycznej Zamawiającego przy użyciu jakiejkolwiek metody, która nie została wyraźnie dopuszczona przez Zamawiającego,

	r) przechwytywania, badania lub w inny sposób analizowania jakiegokolwiek komunikacyjnego protokołu używanego przez Zamawiającego, zarówno poprzez analizator sieci, program przechwytujący (sniffer) lub inne urządzenie, s) podejmowania działań, które nie są niezbędne do realizacji zawartych z Zamawiającym Umów.

Oświadczam, że powyższe informacje są prawdziwe

.....

data i podpis osoby upoważnionej do złożenia oświadczenia w imieniu Wykonawcy

PEŁNOMOCNIK
ds. BEZPIECZEŃSTWA
mgr Piotr Trębski