**Załącznik nr** ……… **do Umowy nr** ………………………………..

**ZASADY UDZIELENIA ZDALNEGO DOSTĘPU DO ZASOBÓW**

Niniejszy załącznik ustala zasady udzielenia Wykonawcy zdalnego dostępu do zasobów sieci teleinformatycznej Zamawiającego w celu umożliwienia Wykonawcy realizacji jego zobowiązań wynikających z Umowy.

1. **Udostępnienie**
2. W celu realizacji usług, o których mowa w **§1** umowy nr …………………………………………….z dnia ....................................r. (zwanej dalej Umową Główną) zawartej pomiędzy Zamawiającym - **Szpitale Pomorskie Sp. z o. o.**,a Wykonawcą - ....................................................................., Wykonawca może zastosować metodę Zdalnego Dostępu do infrastruktury teleinformatycznej przedmiotu umowy, który zostanie mu udostępniony przez Zamawiającego niezwłocznie na wezwanie Wykonawcy w terminie szczegółowo uzgodnionym przez Strony.
3. Bezpośredni dostęp do systemów Zamawiającego jest możliwy tylko i wyłącznie po udostępnieniu go przez administratora Zamawiającego i po przekazaniu wymaganych uprawnień i haseł.
4. Zamawiający zapewni sprawne działanie zdalnego dostępu po stronie swojej infrastruktury teleinformatycznej.
5. **Zasady korzystania**
6. Korzystając ze Zdalnego Dostępu Wykonawca:
	1. będzie wykorzystywał Zdalny Dostęp wyłącznie w celu realizacji Umowy Głównej;
	2. nie będzie pozyskiwał, ani przetwarzał żadnych innych danych, za wyjątkiem danych niezbędnych do realizacji Umowy Głównej;
7. Wykonawca może wnioskować o dane logowania tylko i wyłącznie dla osób upoważnionych do przetwarzania danych osobowych, powierzonych do przetwarzania na potrzeby należytej realizacji Umowy Głównej.
8. Zabrania się Wykonawcy przekazywania danych logowania (login lub hasło) innym osobom niż osoby wskazane do realizacji Umowy Głównej.
9. Zdalny Dostęp udostępnia się do realizacji usług wynikających z Umowy Głównej.
10. **Warunki Techniczne do uzyskania Zdalnego Dostępu**
11. Zamawiający zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie bezpiecznego kanału VPN.
12. Na wezwanie Wykonawcy, Zamawiający przekaże osobie realizującej wynikające z zapisów Umowy Głównej prace, identyfikator użytkownika (login) wraz z hasłem 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 Umowy Głównej.
13. Wszystkie dane dotyczące parametrów logowania zostaną przekazane przez Zamawiającego na indywidualne konta pocztowe e-mail osób wskazanych przez Wykonawcę dla celów realizacji usług serwisowych i gwarancyjnych. Tą samą drogą dostarczone zostanie również przez Zamawiającego oprogramowanie klienta VPN lub klienta terminalowego. Oprogramowanie zostanie zainstalowane na komputerach użytkowników staraniem Wykonawcy.
14. **Cyberbezpieczeństwo**
15. Zamawiający jest operatorem usługi kluczowej w zakresie:
	1. Udzielanie świadczeń opieki zdrowotnej przez podmiot leczniczy,
	2. Obrocie i dystrybucji produktów leczniczych.
16. Zgodnie z ustawą z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa Wykonawca jest zobowiązany do zgłaszania:
	1. incydentów RODO na adres mailowy: iod@szpitalepomrskie.eu lub osobiście u IOD,
	2. incydentów poważnych niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia na adres mailowy: incydent@szpitalepomorskie.eu oraz kontaktKSC@szpitalepomorskie.eu lub osobiście w Dziale Informatyki Zamawiającego.
17. Wykonawca przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu poważnego.
18. Pracownicy Wykonawcy współdziałają podczas obsługi incydentu poważnego i incydentu krytycznego z Działem Informatyki Zamawiającego oraz z CSIRT NASK oraz sektorowym zespołem cyberbezpieczeństwa, przekazując niezbędne dane, w tym dane osobowe.
19. Pracownik Wykonawcy obsługujący incydent przekazuje, w niezbędnym zakresie, w zgłoszeniu, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań CSIRT NASK oraz sektorowego zespołu cyberbezpieczeństwa.
20. W zgłoszeniu Pracownik Wykonawcy oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.
21. Wykonawca usuwa podatności w systemie informatycznym dostarczonym zgodnie z Umową Główną. Usunięciu podlegają podatności dla których w trakcie koordynacji obsługi incydentu poważnego, incydentu istotnego lub krytycznego, CSIRT NASK wystąpi do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie operatora usługi kluczowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, incydentu istotnego lub krytycznego.
22. Wykonawca zastosuje mechanizmy zapewniające poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informatycznym dostarczonym zgodnie z Umową Główną oraz podczas zdalnego dostępu do zasobów.
23. Wykonawca będzie dbać o aktualizację oprogramowania.
24. Wykonawca skonfiguruje dostarczane systemy tak by pobierały czas z serwera NTP Zamawiającego.
25. Wykonawca niezwłocznie podejmie działania po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa.
26. Progi uznania incydentu za poważny:

|  |  |
| --- | --- |
| Incydent dotyczący udzielania świadczenia opieki zdrowotnej | Incydent doprowadził do braku dostępności usługi powyżej 24 godzin.Incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu,c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby,d) brak poufności danych przetwarzanych w usłudze, e) brak integralności danych przetwarzanych w usłudze. |
| Incydent dotyczący obrotu i dystrybucji produktów leczniczych | Incydent doprowadził do braku dostępności usługi powyżej 24 godzin.Incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu,c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby,d) brak poufności danych przetwarzanych w usłudze, e) brak integralności danych przetwarzanych w usłudze. |