**UMOWA NR ……/2022**

na poprawę cyberbezpieczeństwa w SPZOZ w Łukowie

zawarta w dniu ……………….

pomiędzy:

**Samodzielnym Publicznym Zakładem Opieki Zdrowotnej w Łukowie**, 21 – 400 Łuków, ul. Doktora Andrzeja Rogalińskiego 3, wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej w Sądzie Rejonowym Lublin-Wschód w Lublinie z siedzibą w Świdniku VI Wydziale Gospodarczym Krajowego Rejestru Sądowego, KRS Nr 000056773, REGON: 000306472, NIP: 825 – 17 – 11 – 719, zwanym dalej „Zamawiającym” reprezentowanym przez działających na podstawie pełnomocnictwa:

Mariusz Furlepa – Dyrektor SPZOZ w Łukowie

a

…………………………………………………………………………………………………..,   
NIP ………………., REGON …………….., zwanym dalej „Wykonawcą” reprezentowanym przez:

1. ……………………..

w wyniku udzielenia zapytania ofertowego nr SI/9/2022 na Poprawę Cyberbezpieczeństwa w SPZOZ w Łukowie, została zawarta umowa o następującej treści:

**1.**

**PRZEDMIOT UMOWY**

1. Przedmiotem Umowy jest realizacja zadań polegających na:

- Zadanie 1: wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji,

- Zadanie 2: przeprowadzeniu audytu spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa przez operatora usługi kluczowej,

- Zadanie 3: przeprowadzeniu szkolenia z zakresu cyberbezpieczeństwa,

- Zadanie 4: wykonaniu testów podatności infrastruktury teleinformatycznej wraz z przygotowaniem raportu z opisem podatności i rekomendacjami.

Szczegółowy opis Przedmiotu Umowy określony został w załączniku nr 1 do Umowy, stanowiącym integralną część niniejszej umowy.

1. Czynności objęte Przedmiotem Umowy realizowane będą w następujących lokalizacjach Samodzielnego Publicznego Zespołu Zakładów Opieki Zdrowotnej w Łukowie:

* Samodzielny Publiczny Zakład Opieki Zdrowotnej w Łukowie, 21-400 Łuków, ul. Doktora Andrzeja Rogalińskiego 3.

**2.**

**TERMIN REALIZACJI**

1. Wykonawca wykona Przedmiot Umowy określony w 1 w terminie nieprzekraczalnym terminie do dnia 20 listopada 2022 r, w tym:

* Spotkanie koordynacyjne Stron i szczegółowe zaplanowanie realizacji usługi - do 7 dni roboczych od dnia zawarcia Umowy,
* Zadanie1: Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji - do10 listopada 2022 roku,
* Zadanie 2: Przeprowadzenie audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego po wdrożeniu przez Zamawiającego czynności podnoszących poziom bezpieczeństwa systemów teleinformatycznych - do 7 dni roboczych od dnia powiadomienia przez Zamawiającego Wykonawcy o gotowości do poddania się Audytowi. Powiadomienie Wykonawcy przez Zamawiającego o gotowości do poddania się Audytowi powinno nastąpić nie później niż do dnia 10 listopada 2022 r.

Sporządzenie Raportu z Audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego i przekazanie go Zamawiającemu - do 7 dni roboczych od dnia zakończenia Audytu.

* Zadanie 3: Przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa, zgodnie ze szczegółowym zakresem określonym w załączniku do Umowy, w terminie do 21 dni od dnia zawarcia Umowy.
* Zadanie 4: Wykonanie testów podatności infrastruktury teleinformatycznej wraz z przygotowaniem raportu z opisem podatności i rekomendacjami w terminie 21 dni od dnia zawarcia Umowy.

1. Terminy wykonania Przedmiotu Umowy określone w §2 ust 1. mogą ulec odpowiedniemu przesunięciu o czas trwania opóźnień, wynikających z okoliczności zaistniałych po stronie Zamawiającego.

**§3.**

**WYNAGRODZENIE**

1. Za pełne i prawidłowe wykonanie Przedmiotu Umowy Wykonawca otrzyma wynagrodzenie w kwocie: ………… **zł netto *(słownie:*** *…………* plus należny podatek VAT, co stanowi kwotę **brutto:** …….….. ***(słownie:*** *……………………….), w tym za:* Zadanie1 …….., Zadanie 2………, Zadanie 3………, Zadanie4……..*.*
2. Wynagrodzenie Wykonawcy jest ostateczne i obejmuje wszystkie koszty, jakie mogą powstać w związku z realizacją Przedmiotu Umowy, w tym wszelkie opłaty i podatki.
3. Podstawą do wystawienia przez Wykonawcę faktury będzie Protokół odbioru każdego z elementów wskazanych w Umowie, jako Zadania, podpisany przez Zamawiającego bez zastrzeżeń.
4. W ramach realizacji Przedmiotu Umowy Wykonawca wystawi oddzielne faktury dla każdego z przewidzianych w Umowie Zadań.
5. Wynagrodzenie będzie płatne w terminie do 14 dni od daty wpływu do Zamawiającego prawidłowo wystawionej faktury.
6. Wynagrodzenie będzie płatne przelewem na konto Wykonawcy wskazane na fakturze.
7. Za dzień zapłaty Strony uznają dzień obciążenia rachunku bankowego Zamawiającego.
8. Zamawiający na podstawie art. 106n ust. 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług udziela Wykonawcy zgody na wystawianie i przesyłanie z adresu e‑mail: ………………. faktur, duplikatów faktur oraz ich korekt, a także not obciążeniowych i not korygujących w formacie pliku elektronicznego PDF na adres e-mail: …………………...

**§4.**

**ZESPÓŁ**

1. Wykonawca oświadcza, że dysponuje odpowiednim potencjałem techniczno–organizacyjnym, personelem posiadającym odpowiednie kwalifikacje oraz wiedzą i doświadczeniem pozwalającymi na należytą realizację przedmiotu Umowy.
2. Wykonawca zapewni Zespół specjalistów dedykowanych do realizacji Umowy, zgodnie z ofertą. Wymagania w zakresie Zespołu Wykonawcy oraz skład zespołu określone są w Załączniku nr 2 do Umowy. Osoby wyznaczone do wykonania Umowy posiadają kwalifikacje, wiedzę i doświadczenie zgodne z warunkami określonymi w Załączniku nr 2do Umowy.
3. W trakcie obowiązywania Umowy Wykonawcy przysługiwać będzie prawo do zastępowania za zgodą Zamawiającego członków personelu Wykonawcy innymi osobami, o co najmniej takich samych odpowiednio kwalifikacjach lub doświadczeniu jak określone w Załączniku nr 1do Umowy. Zamawiający dokona akceptacji zmiany osób wskazanych do realizacji Umowy w ciągu 3 dni od zgłoszenia jej przez Wykonawcę.
4. W przypadku zmiany osoby wskazanej na danym stanowisku, danej roli, osoba zastępująca musi posiadać odpowiednio doświadczenie zawodowe i/lub kwalifikacje nie gorsze niż osoba zastępowana.
5. Zasady opisane w ust. 3 i 4 będą miały zastosowanie również w przypadku wskazania przez Wykonawcę dodatkowych osób do skierowanych do realizacji zadań dla których wymagania minimalne zostały określone w Załączniku nr 2 do Umowy.
6. Zamawiający ma prawo zażądać zmiany członka personelu Wykonawcy w przypadku pojawienia się uzasadnionych zastrzeżeń, co do jego kwalifikacji, wiedzy, rzetelności lub terminowości wykonywania obowiązków. Zamawiający zobowiązany jest przekazać zastrzeżenia w formie pisemnej. W takim przypadku Wykonawca dokona zmiany członka personelu na nowego, spełniającego wymagania określone w Załączniku nr 2 do Umowy, nie później niż w terminie 5 dni od zgłoszenia zastrzeżeń przez Zamawiającego. Wykonawca zobowiązany jest poinformować Zamawiającego o zaprzestaniu wykonywania prac przez danego członka personelu Wykonawcy, w terminie 7 dni od nastąpienia tego zdarzenia. Każda zmiana personelu, o której mowa powyżej, skutkuje odbiorem lub nadaniem uprawnień do systemów przez Zamawiającego.
7. Zmiana osób, o której mowa powyżej, nie stanowi zmiany Umowy i nie wymaga zawarcia aneksu do Umowy. Wykonawca jest zobowiązany do niezwłocznego poinformowania Zamawiającego o powyższej zmianie w formie pisemnej oraz zapewnienia transferu wiedzy pomiędzy osobami zastępowaną i zastępującą, jak również realizacji innych obowiązków wynikających z Umowy względem nowego członka personelu.
8. Osobami uprawnionymi do bieżących kontaktów w ramach realizacji przedmiotu umowy oraz do odbioru Raportu i podpisywania protokołów są osoby:
   1. po stronie Zamawiającego: Pan/i Tomasz Buziak e-mail: t.buziak@spzoz.lukow.pl
   2. po stronie Wykonawcy: Pan/i ……………… e-mail: ………………………….

**§5.**

**REALIZACJA UMOWY**

1. Zamawiający zobowiązuje się do współdziałania z Wykonawcą, w szczególności poprzez:
2. współpracę w zakresie planowania przez Wykonawcę czynności w zakresie realizacji przedmiotu Umowy,
3. umożliwienie Wykonawcy wykonania przedmiotu Umowy określonego w §1 ust. 1 Umowy.
4. Strony zgodnie ustalają, że na potrzeby realizacji Umowy do wymiany korespondencji będą używać drogi elektronicznej w postaci przesyłania wiadomości e-mail opatrzonych każdorazowo imieniem i nazwiskiem osoby wysyłającej wiadomość bez konieczności podpisywania korespondencji kwalifikowanym podpisem elektronicznym. Na potrzeby realizacji Umowy Strony udostępniają adresy e-mail określone w §4 ust. 8. Strony gwarantują, że powyższymi adresami posługiwać się mogą wyłącznie osoby upoważnione do kontaktów z drugą Stroną.
5. Wykonawca gwarantuje, że jego usługi będą świadczone w profesjonalny sposób, według odpowiedniej wiedzy i doświadczenia, z najwyższą starannością wymaganą od czołowych przedsiębiorstw IT w Polsce i efektywnością, oraz że wykona zlecone mu prace terminowo i zgodnie i obowiązującym stanem prawnym.
6. Wykonawca uprawniony będzie do realizacji Przedmiotu Umowy w siedzibie Zamawiającego lub zdalnie po uzyskaniu pisemnej zgody Zamawiającego.
7. Wykonawca dołoży wszelkich starań w celu uniknięcia wpływu testów na prace testowanych systemów. Termin i zakres prowadzenia prac będzie każdorazowo uzgadniany z Zamawiającym, tak aby zminimalizować potencjalne skutki testów.
8. Wykonawca ponosi całkowitą odpowiedzialność za swoje działania lub zaniechania związane z realizacją Umowy, chyba że szkoda nastąpiła wskutek siły wyższej albo wyłącznie z winy Zamawiającego lub osoby trzeciej za którą Wykonawca nie ponosi odpowiedzialności.
9. Wykonawca nie jest uprawniony do wprowadzania jakichkolwiek zmian do systemów teleinformatycznych Zamawiającego bez pisemnej zgody Zamawiającego, w szczególności Wykonawca zobowiązuje się nie wprowadzać żadnych zmian do baz danych wykorzystywanych przez Zamawiającego.
10. Zawierając Umowę Wykonawca zobowiązuje się jednocześnie do zawarcia z Zamawiającym umowy powierzenia przetwarzania danych osobowych, na podstawie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 2016.119.1), której wzór stanowi Załącznik nr 4 do Umowy.

**§6.**

**ODBIÓR PRAC**

1. Wykonawca przekazuje Zamawiającemu informację o zakończeniu poszczególnego Zadania wraz z dołączonym protokołem odbioru na wskazany w Umowie adres mailowy.
2. Zamawiający w terminie do 3 dni roboczych zaakceptuje przekazane informacje albo zgłosi uwagi, przesyłając je na adres określony w §4 ust. 8 pkt 2).
3. W przypadku zgłoszenia uwag przez przedstawicieli Zamawiającego wskazanych w §4 ust. 8 pkt 1), Wykonawca odpowie na zgłoszone przez Zamawiającego uwagi i w przypadku uwzględnienia uwag Zamawiającego ponownie przedstawi Zamawiającemu do akceptacji poprawione informacje, nie późnej niż w terminie 5 dni roboczych od otrzymania uwag od Zamawiającego.
4. W przypadku zgłoszenia przez Zamawiającego dalszych uwag do wykonania przedmiotu Umowy, postanowienia ust. 3 i 4 stosuje się odpowiednio.
5. Odbiór poszczególnych Zadań nastąpi w formie Protokołu odbioru, podpisanego przez Zamawiającego bez zastrzeżeń.
6. Za termin wykonania przedmiotu umowy strony uznają dzień podpisania przez Zamawiającego protokołu odbioru bez zastrzeżeń.

**§7.**

**KARY UMOWNE**

1. Wykonawca może zostać zobligowany przez Zamawiającego do zapłaty kar umownych:
2. w przypadku odstąpienia od umowy przez Wykonawcę lub przez Zamawiającego z przyczyn leżących po stronie Wykonawcy - w wysokości 10% wynagrodzenia brutto, o którym mowa w §3 ust. 1,
3. w przypadku zwłoki w wykonaniu umowy ponad termin określony w §2 ust. 1 - w wysokości 0,5 % wynagrodzenia brutto, o którym mowa w §3 ust. 1 za każdy dzień zwłoki z zastrzeżeniem §2 ust. 2 Umowy.
4. za każdy stwierdzony przypadek ujawnienia jakiejkolwiek informacji lub innego naruszenia bezpieczeństwa informacji, w okresie obowiązywania umowy, jak też i po jej wygaśnięciu lub rozwiązaniu, w tym niewykonanie obowiązku określonego w §11 ust. 12 - w wysokości do 20% wynagrodzenia brutto, o którym mowa w §3 ust. 1. Wysokość kary jest ustalana proporcjonalnie do wyrządzonej szkody.
5. W przypadku niedokonania przez Wykonawcę na żądanie Zamawiającego zmiany członka personelu, zgodnie z warunkami określonymi w §4 oraz Załącznika nr 1 do Umowy, w terminie 14 dni od dnia zgłoszenia zastrzeżeń przez Zamawiającego, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 300 zł za każdy dzień zwłoki w wykonaniu powyższego obowiązku.
6. Zamawiający może zostać zobligowany przez Wykonawcę do zapłaty kar umownych:

1) w przypadku odstąpienia od umowy przez Zamawiającego lub przez Wykonawcę z przyczyn leżących po stronie Zamawiającego - w wysokości 10% wynagrodzenia brutto, o którym mowa w §3 ust. 1.

2) W przypadku braku współdziałania Zamawiającego z Wykonawcą skutkujący przekroczeniem terminu realizacji umowy.

3) W przypadku naruszenia zobowiązań w zakresie poufności danych.

1. W przypadku realizacji Umowy przez którąkolwiek z osób wchodzących w skład personelu, która nie spełnia wymagań określonych w Opisie Przedmiotu Zamówienia albo jej zmiana nie została zaakceptowana przez Zamawiającego, Wykonawca zapłaci Zamawiającemu karę w wysokości 300 zł za każdy dzień świadczenia usługi przez Wykonawcę z udziałem ww. osoby.
2. Kary umowne mogą podlegać sumowaniu oraz mogą być naliczane niezależnie od siebie z tym zastrzeżeniem, że jeśli to samo działanie lub zaniechanie Wykonawcy wypełnia przesłanki do naliczenia dwóch lub więcej kar umownych wskazanych w Umowie, to Zamawiający naliczy karę wyższą, nie może on jednak nałożyć więcej niż jednej kary za to samo działanie czy zaniechanie. Kary będą naliczane za każdy przypadek naruszenia Umowy odrębnie.
3. W przypadku zaistnienia przesłanek naliczenia kary umownej, Zamawiający wystawi notę obciążeniową z terminem płatności nie krótszym niż 7 dni.
4. Jeżeli szkoda przewyższy wysokość kary umownej, Zamawiającemu przysługiwać będzie roszczenie o zapłatę odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych.
5. Wykonawca ponosi odpowiedzialność za szkody wyrządzone Zamawiającemu przy wykonywaniu lub w związku z wykonywaniem postanowień umowy. Kary umowne wskazane powyżej przysługują Zamawiającemu także w przypadku odstąpienia od umowy lub jej wypowiedzenia, niezależnie od kary umownej z tytułu odstąpienia lub wypowiedzenia umowy.
6. Łączna wysokość kar umownych ograniczona jest do 50 % kwoty brutto określonej w §3 ust. 1.

**§8.**

**ODSTĄPIENIE OD UMOWY I WYPOWIEDZENIE**

1. Zamawiającemu przysługuje prawo do odstąpienia od umowy w przypadku gdy Wykonawca nie rozpoczął realizacji umowy lub nie kontynuuje jej niezwłocznie po wezwaniu złożonym na piśmie przez Zamawiającego.
2. Zamawiającemu przysługuje prawo do wypowiedzenia umowy w trybie natychmiastowym, bez zachowania okresu wypowiedzenia w następujących przypadkach:
3. w przypadku niewykonania lub nienależytego wykonywania przedmiotu umowy przez Wykonawcę – w takim wypadku Zamawiający wyznaczy Wykonawcy dodatkowy 5-dniowy termin na wykonanie zobowiązania. Jeśli Wykonawca nie rozpocznie w ww. terminie wykonywania przedmiotu umowy w sposób należyty, Zamawiający ma prawo wypowiedzieć umowę ze skutkiem na dzień złożenia wypowiedzenia,
4. naruszył bezpieczeństwo informacji lub zasady z nim związane.
5. W przypadku zwłoki w realizacji przedmiotu Umowy przekraczającej 7 dni ponad termin wskazany w §2 ust. 1 Zamawiający może, niezależnie od nałożenia na Wykonawcę kar umownych, odstąpić od umowy w całości lub w części. Termin ten ulega odpowiedniemu przesunięciu o czas trwania opóźnień, które wynikły z winy Zamawiającego.
6. Oświadczenie o odstąpieniu lub wypowiedzeniu powinno być złożone na piśmie i zostać dostarczone drugiej Stronie.
7. Zamawiający może odstąpić od Umowy w terminie 30 dni od daty zaistnienia zdarzenia stanowiącego podstawę do odstąpienia.
8. Odstąpienie od umowy nie wpływa na obowiązek zachowania poufności informacji.
9. W razie odstąpienia od umowy lub jej wypowiedzenia, Zamawiający – w ramach należnego Wykonawcy wynagrodzenia - nabywa autorskie prawa majątkowe i zależne prawa autorskich do utworów oraz utworów i ich nośników, odnośnie do których Zamawiający praw nie nabył, w zakresie określonym w §9, z chwilą złożenia oświadczenia o odstąpieniu lub wypowiedzeniu.
10. Siła wyższa:
11. Żadna Strona nie będzie odpowiedzialna za niewykonanie swoich zobowiązań w ramach umowy w stopniu, w jakim opóźnienie w jej działaniu lub inne niewykonanie jej zobowiązań jest wynikiem Siły Wyższej,
12. Dla potrzeb umowy „Siła Wyższa” oznacza wydarzenie nadzwyczajne pozostające poza kontrolą Strony, występujące po podpisaniu umowy przez obie Strony, przeszkadzające racjonalnemu wykonaniu przez tę Stronę jej obowiązków, nie obejmujące winy własnej lub nienależytej staranności tej Strony i nieprzewidywalne w dacie zawarcia umowy.
13. Jeżeli Siła Wyższa spowoduje niewykonanie lub nienależyte wykonanie zobowiązań wynikających z umowy:
14. Strona – o ile będzie to możliwe - zawiadomi w terminie 2 dni na piśmie drugą Stronę o powstaniu i zakończeniu tego zdarzenia, w miarę możliwości przedstawiając stosowną dokumentację w tym zakresie,
15. Strona niezwłocznie przystąpi do dalszego wykonywania umowy,
16. Strony uzgodnią sposób postępowania wobec tego zdarzenia oraz terminy wykonywania umowy.
17. Jeżeli Siła Wyższa spowoduje niewykonanie lub nienależyte wykonanie zobowiązań wynikających z umowy przez okres powyżej trzech (3) tygodni, Strony spotkają się i w dobrej wierze rozpatrzą celowość i warunki rozwiązania umowy.

**§9.**

**PRAWA AUTORSKIE**

1. Wykonawca oświadcza, że będą mu przysługiwały autorskie prawa majątkowe i prawa zależne do wszelkich utworów, które powstaną w wyniku wykonania Umowy.
2. Wykonawca, z dniem podpisania protokołu odbioru Raportu, przenosi na Zamawiającego autorskie prawa majątkowe do Raportu, na następujących polach eksploatacji:
3. w zakresie utrwalania i zwielokrotniania Raportu, - wytwarzanie określoną techniką egzemplarzy, w tym drukarską reprograficzną, elektroniczną, fotograficzną, cyfrową, audiowizualną, technikami multimedialnymi oraz zapisu magnetycznego obejmujące trwałe lub czasowe utrwalanie lub zwielokrotnianie w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie, niezależnie od formatu, systemu lub standardu bez ograniczeń co do ilości egzemplarzy oraz korzystania i rozporządzania tymi egzemplarzami;
4. w zakresie obrotu oryginałem albo egzemplarzami, na których Raportu utrwalono - wprowadzenie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;
5. w zakresie rozpowszechniania Raportu, w sposób inny niż określony w pkt 2 - publiczne wykonanie, wyświetlenie, odtworzenie, nadanie i reemitowanie, a także publiczne udostępnienie Raportu, w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym.
6. Wykonawca przenosi na rzecz Zamawiającego, z chwilą podpisania przez Zamawiającego protokołu odbioru Raportu, prawo zezwalania na wykonanie zależnego prawa autorskiego, w tym do rozporządzania i korzystania z opracowań Raportu, w nieograniczonym zakresie, w szczególności w zakresie pól eksploatacyjnych wskazanych w ust. 2.
7. Z chwilą podpisania przez Zamawiającego protokołu odbioru Raportu, Zamawiający nabywa na własność egzemplarze Raportu, przekazane przez Wykonawcę oraz nośniki, na których Raport utrwalono.
8. Zamawiający nie ponosi odpowiedzialności za naruszenie autorskich praw majątkowych lub osobistych wobec osób trzecich. Wykonawca zobowiązuje się do nieodwołalnego i bezwarunkowego zwolnienia Zamawiającego, na pierwsze żądanie, z wszelkich roszczeń, wynikających z naruszenia majątkowych i osobistych praw autorskich, do którego doszło z przyczyn leżących po stronie Wykonawcy.
9. Wykonawca oświadcza, że przygotowany przez niego Raport będzie oryginalny i nie będzie naruszał praw osób trzecich oraz będzie wolny od wad. Wykonawca zobowiązuje się, że w momencie przekazywania Raportu Zamawiającemu będzie wyłącznym ich dysponentem majątkowym praw autorskich.
10. Przeniesienie autorskich praw majątkowych zostaje dokonane na czas nieokreślony i jest nieograniczone terytorialnie.
11. W przypadku ujawnienia nowego pola eksploatacji mającego znaczenie dla Zamawiającego, Strony ustalają, że Wykonawca na wezwanie Zamawiającego przeniesie na Zamawiającego, w terminie 14 dni od doręczenia Wykonawcy wezwania, autorskie prawa majątkowego do Raportu oraz prawo zezwalania na wykonywanie praw zależnych do Raportu na nowym polu eksploatacji, na zasadach określonych w niniejszej umowie. Przeniesienie praw, o których mowa w zdaniu poprzednim, zostanie dokonane na rzecz Zamawiającego w ramach wynagrodzenia przewidzianego niniejszą umową.

**§10.**

**ROZSTRZYGANIE SPORÓW**

1. Ewentualne spory wynikłe na tle realizacji Umowy Strony będą starały się załatwiać polubownie. W przypadku braku porozumienia sądem właściwym miejscowo do rozstrzygania sporów będzie sąd właściwy dla siedziby Zamawiającego.

**§11.**

**OCHRONA INFORMACJI**

1. Informacją w rozumieniu Umowy są wszelkie informacje, dokumenty lub dane przekazane Wykonawcy przez Zamawiającego, uzyskane przez Wykonawcę w związku z realizacją Umowy oraz wytworzone przez Wykonawcę na potrzeby realizacji Umowy.
2. Wykonawca może przetwarzać powierzone mu przez Zamawiającego informacje przez okres obowiązywania Umowy.
3. Wykonawca zobowiązuje się po zakończeniu realizacji Umowy do zwrotu Zamawiającemu wszelkich udostępnionych oraz wytworzonych przez siebie w związku z realizacją Umowy informacji, wraz z nośnikami. W przypadku utrwalenia na nośnikach należących do Wykonawcy informacji uzyskanych w związku z realizacją Umowy, Wykonawca zobowiązuje się do usunięcia z nośników tych informacji, w tym również sporządzonych kopii zapasowych, oraz zniszczenia wszelkich danych, dokumentów mogących posłużyć do odtworzenia, w całości lub części, informacji.
4. Wykonawca zobowiązuje się do przestrzegania wytycznych Zamawiającego o ochronie udostępnianych informacji.
5. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji, a także sposobów zabezpieczenia informacji, zarówno w trakcie trwania niniejszej Umowy, jak i po jej wygaśnięciu lub rozwiązaniu. Wykonawca ponosi pełną odpowiedzialność za zachowanie w tajemnicy ww. informacji przez osoby realizujące Umowę.
6. Wykonawca zobowiązany jest do zastosowania wszelkich niezbędnych środków technicznych i organizacyjnych zapewniających ochronę przetwarzania informacji, a w szczególności powinien zabezpieczyć informacje przed ich udostępnieniem osobom nieuprawnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem postanowień Umowy, zmianą, utratą, uszkodzeniem, zniszczeniem lub kradzieżą.
7. Wykonawca zobowiązuje się do dołożenia najwyższej staranności w celu zabezpieczenia informacji przed bezprawnym dostępem, rozpowszechnianiem lub przekazaniem osobom trzecim.
8. Wykonawca zobowiązany jest zapewnić wykonanie obowiązków w zakresie bezpieczeństwa informacji, w szczególności dotyczącego zachowania w tajemnicy informacji, także przez jego pracowników oraz osoby, które realizują Umowę w imieniu Wykonawcy. Odpowiedzialność za naruszenie powyższego obowiązku spoczywa na Wykonawcy. Naruszenie bezpieczeństwa informacji, w szczególności ujawnienie jakiejkolwiek informacji w okresie obowiązywania Umowy, uprawnia do odstąpienia przez Zamawiającego od Umowy.
9. Wykonawca może udostępniać informacje jedynie tym swoim pracownikom lub osobom współpracującym na podstawie umów cywilnoprawnych, którym będą one niezbędne do wykonania powierzonych im czynności i tylko w zakresie, w jakim muszą mieć do nich dostęp dla celów określonych w niniejszej Umowie.
10. Wykonawca oraz inne osoby, które realizują Umowę w imieniu Wykonawcy, zobowiązane są przed przystąpieniem do prac do podpisania oświadczenia o zachowaniu poufności informacji, którego wzór stanowi Załącznik nr 3 do Umowy. Podpisane oświadczenie należy przekazać Zamawiającemu przed rozpoczęciem realizacji Umowy przez ww. pracowników.
11. Wykonawca ponosi wszelką odpowiedzialność, tak wobec osób trzecich, jak i wobec Zamawiającego, za szkody powstałe w związku z nienależytą realizacją obowiązków dotyczących zapewnienia bezpieczeństwa informacji.
12. Wykonawca zobowiązuje się do ścisłego przestrzegania warunków niniejszej Umowy, które wiążą się z ochroną informacji, w szczególności nie może bez pisemnego upoważnienia Zamawiającego wykorzystywać informacji w celach niezwiązanych z realizacją Umowy.
13. W przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji lub z naruszeniem obowiązków wynikających z Umowy, Zamawiający może przeprowadzić kontrolę wykonywanych przez Wykonawcę czynności. Kontrola może być realizowana przez Zamawiającego lub podmioty przez niego uprawnione. Wykonawca zobowiązany jest współpracować z Zamawiającym w odpowiednim zakresie z podmiotami przeprowadzającymi kontrolę. Wyniki kontroli zostaną przekazane Wykonawcy po jej zakończeniu. Zamawiający może wskazać niezbędne działania, jakie Wykonawca musi podjąć w celu wprowadzenia określonych zmian lub podjęcia określonych czynności.
14. Wykonawca zobowiązany jest do natychmiastowego powiadamiania o nieuprawnionym ujawnieniu lub udostępnieniu informacji oraz o innym naruszeniu bezpieczeństwa informacji, a następnie raportowania Zamawiającemu o podjętych działaniach w powyższym zakresie:
15. telefonicznie, na numer telefonu: 25 7980409 .
16. na adres email: t.buziak@spzoz.lukow.pl .

Powiadomienie dokonane telefonicznie musi zostać potwierdzone poprzez sposób wskazany w pkt 2) w terminie jednej godziny od dokonania powiadomienia.

1. Wykonawca nie może zwielokrotniać, rozpowszechniać, korzystać w celach niezwiązanych z realizacją Umowy oraz ujawniać informacji osobom trzecim, bez uzyskania w powyższym zakresie pisemnej zgody Zamawiającego, o ile takie informacje nie zostały już podane do publicznej wiadomości lub nie są publicznie dostępne.
2. Wykonawca zobowiązany jest:
3. zapewnić kontrolę nad tym, jakie informacje, kiedy, przez kogo oraz komu są przekazywane;
4. zapewnić, aby osoby, o których mowa w pkt 1, zachowywały w tajemnicy informacje oraz sposoby ich zabezpieczeń.
5. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji uzyskanych przez niego w związku z zawarciem Umowy. Wykonawca ponosi pełną odpowiedzialność za zachowanie w tajemnicy ww. informacji przez podmioty, przy pomocy których wykonuje Umowę.
6. Wykonawca zobowiązany jest zapewnić bezpieczeństwo informacji przed wystąpieniem zagrożeń, w szczególności poprzez:
7. zastosowanie firewall oraz oprogramowania antyspamowego i antywirusowego,
8. zapewnienie kontroli dostępu do powierzonych zasobów Zamawiającego,
9. uniemożliwienie dostępu do haseł do zasobów informatycznych Zamawiającego przez osoby nieuprawnione wraz z ich cykliczną zmianą,
10. zastosowanie zabezpieczeń ochrony fizycznej.

**§12.**

**ZMIANY DO UMOWY**

1. O ile Umowa nie stanowi inaczej, zmiany treści Umowy mogą być dokonywane wyłącznie w formie aneksu podpisanego przez obie Strony, pod rygorem nieważności w zakresie:
2. zmiany szczegółowych zasad wykonywania przedmiotu Umowy określonych w załącznikach do Umowy, spowodowane zmianami organizacyjnymi u Zamawiającego;
3. zmiany zakresu realizacji Przedmiotu Umowy, w przypadku wystąpienia zmiany okoliczności powodującej, że:
   1. realizacja części Przedmiotu Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawierania Umowy,
   2. realizacja części Przedmiotu Umowy nie jest zasadna na skutek zmiany lub planowanej zmiany powszechnie obowiązujących przepisów prawa.
4. zmiany postanowień Umowy będące następstwem zmian powszechnie obowiązujących przepisów prawa, których wejście w życie lub zmiana nastąpiły po wszczęciu postępowania o udzielenie zamówienia publicznego, a które mają wpływ na realizację Umowy i z których treści wynika konieczność lub zasadność wprowadzenia zmian postanowień Umowy; powyższa zmiana dotyczy także zmiany postanowień Umowy w związku ze zmianą przepisów dotyczących ochrony danych osobowych, w szczególności w zakresie obowiązku spełniania przez Wykonawcę wymagań określonych przez Zamawiającego, poddania się kontroli oraz odstąpienia od Umowy przez Zamawiającego w związku z nieprzestrzeganiem przez Wykonawcę obowiązków związanych z ochroną danych osobowych lub poddaniu się kontroli;
5. zmiany terminu wykonania Umowy spowodowane zmianą powszechnie obowiązujących przepisów prawa, których wejście w życie lub zmiana nastąpiły po wszczęciu postępowania o udzielenie zamówienia publicznego, a które mają wpływ na realizację Umowy;
6. niezbędna jest zmiana sposobu wykonania zobowiązania, o ile zmiana taka jest konieczna w celu prawidłowego wykonania Przedmiotu Umowy;
7. niezbędna jest zmiana terminu realizacji Umowy w przypadku zaistnienia okoliczności lub zdarzeń uniemożliwiających realizację Umowy w wyznaczonym terminie, na które obie Strony nie miały wpływu. W takim przypadku termin realizacji umowy zostanie odpowiednio wydłużony o czas trwania przyczyny uniemożliwiającej realizację Umowy;
8. Zmiany, o których mowa w ust. 1 pkt 1 - 6, nie mogą spowodować zwiększenia łącznego wynagrodzenia brutto, o którym mowa w §3 ust. 1.

**§13.**

**POSTANOWIENIA KOŃCOWE**

1. Wszelkie zmiany i uzupełnienia Umowy, jej wypowiedzenie, rozwiązanie za zgodą obu Stron lub odstąpienie od niej dokonywane będą w formie pisemnej pod rygorem nieważności.
2. Wykonawca bez zgody podmiotu tworzącego Zamawiającego nie może dokonać cesji wierzytelności.
3. Dla potrzeb Umowy Strony ustalają, że ilekroć w umowie jest mowa o dniach roboczych należy przez to rozumieć dni tygodnia przypadające od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
4. W trakcie wykonania przedmiotu Umowy Wykonawca będzie odpowiadać jak za swoje własne czyny za wszelkie czyny lub zaniechania swoich pracowników lub innych osób, którym Wykonawca powierzy za zgodą Zamawiającego wykonanie czynności związanych z realizacją Przedmiotu Umowy.
5. Niewykonanie przez Zamawiającego któregokolwiek z uprawnień przysługujących mu na podstawie Umowy nie może w żadnym razie być uważane za zrzeczenie się tego uprawnienia, ani zrzeczenie się innych uprawnień wynikających z postanowień Umowy.
6. Umowę sporządzono w 3 jednobrzmiących egzemplarzach: jeden dla Wykonawcy i dwa dla Zamawiającego.
7. Załączniki do Umowy stanowią integralną część Umowy.

**WYKONAWCA: ZAMAWIAJĄCY:**

**Spis załączników:**

Załącznik nr 1 – Opis przedmiotu zamówienia,

Załącznik nr 2 – Wykaz osób (zgodnie z ofertą),

Załącznik nr 3 – Wzór oświadczenia o zachowaniu poufności informacji,

Załącznik nr 4 – Wzór umowy powierzenia przetwarzania danych osobowych.

**Załącznik nr 1**

**Do umowy nr ……../2022**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **Ogólna charakterystyka i warunki realizacji zamówienia:**

**Przedmiotem zamówienia jest:**

- wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji,

- przeprowadzenie audytu spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa przez operatora usługi kluczowej,

- przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa,

- wykonanie testów podatności infrastruktury teleinformatycznej wraz z przygotowaniem raportu z opisem podatności i rekomendacjami,

**Zakres przedmiotowy:**

**1. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji:**

Opracowanie wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655) - jeśli dotyczy świadczeniodawcy będącego operatorem usługi kluczowej, o którym mowa w art. 5 tej ustawy, w tym planu odtworzenia po awarii w skład której wchodzą następujące dokumenty:

1. Zakres Systemu Zarządzania Bezpieczeństwem Informacji (ISO 27001) i Ciągłości Działania (ISO 22301).

2. Polityka Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania.

3. Cele Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania.

4. Metodyka szacowania i postępowania z ryzykiem:

• Tabela szacowania ryzyka,

• Tabela postępowania z ryzykiem,

• Raport z szacowania i postępowania z ryzykiem

5. Metodyka szacowania i postępowania z ryzykiem:

• Tabela szacowania ryzyka,

• Tabela postępowania z ryzykiem.

6. Raport z szacowania i postępowania z ryzykiem.

7. Plan szkolenia i uświadamiania.

8. Procedura audytów wewnętrznych.

9. Harmonogram audytów:

• Raport z audytu wewnętrznego,

• Lista kontrolna audytu wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania.

10. Protokół z przeglądu Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania.

11. Procedura działań korygujących, w tym raport z działań korygujących.

12. Procedura identyfikacji wymagań prawnych i regulacyjnych, w tym wykaz wymagań prawnych i regulacyjnych.

Dokumentacja powinna być przygotowana zgodnie z wymogami przepisów:

• Polska norma: PN-EN ISO/IEC 27001:2017-06; Technika informatyczna - Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania,

• Polska norma: PN-EN ISO 22301:2020-04; Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania -- Wymagania.

Wykonawca w ramach wynagrodzenia zobowiązany jest do przeniesienia na Zamawiającego autorskich praw do wszelkiej opracowanej i wytworzonej w ramach niniejszego zamówienia dokumentacji.

**2.** **Audyt KSC:**

Przeprowadzenie audytu spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa przez operatora usługi kluczowej (Zamawiającego) zgodnie z wymogami Ustawy o krajowym systemie cyberbezpieczeństwa, aktów powiązanych oraz szablonem sprawozdania z audytu zgodnego z ustawą o Krajowym Systemie Cyberbezpieczeństwa rekomendowanym przez Ministerstwo Cyfryzacji.

Warunki i zakres przeprowadzenia audytu końcowego w zakresie sprawdzenia bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej z wymaganiami Ustawy:

a) Analiza procesów przetwarzania danych wraz z analizą stanu zabezpieczeń systemowych.

b) Identyfikacja informacji i jej klasyfikacja.

c) Inwentaryzacja zasobów infrastruktury teleinformatycznej, oprogramowania i obszarów bezpiecznych,

d) Identyfikacja i analiza podatności systemów wspomagających świadczenie usługi kluczowej.

Wynikiem analizy musi być pełna lista przeskanowanych pod kątem podatności, systemów zawierająca informacje obejmujące: skanowany system operacyjny, uruchomione na nim usługi, otwarte porty komunikacyjne, listę wykrytych podatności oraz wytyczne dotyczące sposobu usunięcia wykrytych podatności. W celu wykonania powyższych czynności, Wykonawca zobowiązany jest do zapewnienia odpowiedniej licencji na system skanujący.

e) Analiza bezpieczeństwa fizycznego i środowiskowego dla zabezpieczenia realizacji usługi kluczowej.

f) Zarządzanie: ryzykiem, incydentem, podatnościami, środkami technicznymi i organizacyjnymi, systemem monitorowania w trybie ciągłym.

g) Inwentaryzacja procedur.

h) Bezpieczeństwo i ciągłość dostaw i usług od których zależy świadczenie usługi kluczowej.

i) Przegląd dokumentacji związanej z cyberbezpieczeństwem.

j) Zidentyfikowaniu wszelkich niezgodności i wdrożenie działań naprawczych.

Audyt będzie się opierać na wizji lokalnej przeprowadzonej przez wskazane przez Wykonawcę osoby w wybranych lokalizacjach Zamawiającego oraz z wykorzystaniem zdalnego dostępu. Ponadto analiza oparta będzie o wywiad i oświadczenia wskazanych przez Zamawiającego osób.

Audyt bezpieczeństwa, może być przeprowadzony przez:

• jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2022 r. poz. 5 z późn. zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

• co najmniej dwóch audytorów posiadających:

o certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub

o co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub

o co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

• Certified Internal Auditor (CIA);

• Certified Information System Auditor (CISA);

• Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN- EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

• Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

• Certified Information Security Manager (CISM);

• Certified in Risk and Information Systems Control (CRISC);

• Certified in the Governance of Enterprise IT (CGEIT);

• Certified Information Systems Security Professional (CISSP);

• Systems Security Certified Practitioner (SSCP);

• Certified Reliability Professional;

• Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

W celu potwierdzenia spełnienia powyższych wymagań Wykonawca zobowiązany jest do przedłożenia wraz z ofertą w/w certyfikatów.

Wnioski wypływające z audytu powinny wskazywać na potrzebę podjęcia działań korygujących, naprawczych lub doskonalących, jeżeli ma to zastosowanie. Wynikiem audytu będzie sporządzenie przez Wykonawcę raportu, w formie papierowej oraz elektronicznej, określającego konieczne działania, a także zawierającego specyfikację rozwiązań sprzętowych oraz programowych wraz z kompleksową informacją na temat ich wdrożenia i wykorzystania u Zamawiającego celem osiągnięcia zgodności z wymaganiami Ustawy.

Powyższe wytyczne, rekomendacje oraz opisy techniczne rozwiązań (wraz z szacunkową wyceną) dotyczące sposobu wdrożenia odpowiednich, do oszacowanego ryzyka, środków technicznych i organizacyjnych, powinny obejmować m.in.:

• utrzymania i bezpiecznej eksploatacji systemu informacyjnego,

• bezpieczeństwa fizycznego i środowiskowego, uwzględniając kontrolę dostępu,

• bezpieczeństwa oraz ciągłości dostaw i usług, od których zależy świadczenie usługi kluczowej,

• wdrażania, dokumentowania i utrzymywania planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,

• objęcia systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej, systemem monitorowania w trybie ciągłym,

• wdrożenia odpowiednich środków organizacyjnych wymaganych ustawą w celu świadczenia usługi kluczowej,

• wdrożenia wymaganej ustawą dokumentacji systemu cyberbezpieczeństwa.

Obszary Audytu:

a) Ocena skuteczności działania infrastruktury w zakresie urządzeń i konfiguracji w zakresie: ochrony poczty, ochrony sieci, systemów serwerowych, stacji roboczych, systemów bezpieczeństwa,

b) Zarządzanie bezpieczeństwem informacji:

• nośniki wymienne - udokumentowany sposób postępowania,

• zarządzanie tożsamością/dostęp do systemów w zakresie: przydzielanie dostępu, odbieranie dostępu,

• pomieszczenie/pomieszczenia w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwozgodnie z wymogami dla Operatora Usługi Kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa.

c) Monitorowanie i reagowanie na incydenty bezpieczeństwa:

• procedury zarządzania incydentami,

• raportowanie poziomów pokrycia scenariuszami znanych incydentów,

• dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa,

• monitorowanie i wykrycie incydentów bezpieczeństwa,

• Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów.

d) Zarządzanie ciągłością działania:

• konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa,

• raport z przeglądów i testów odtwarzania kopii bezpieczeństwa,

• procedury wykonywania i przechowywania kopii zapasowych,

• strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP),

• procedury utrzymaniowe.

e) Utrzymanie systemów informacyjnych:

• harmonogramy skanowania podatności,

• aktualny status realizacji postępowania z podatnościami,

• procedury związane ze z identyfikowaniem (wykryciem) podatności,

• współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami.

f) Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług:

• polityka bezpieczeństwa w relacjach z dostawcami,

• standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa,

• dostęp zdalny,

• metody uwierzytelnienia.

**3. Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa**

Minimalne wymagania dla programu szkolenia:

• Badanie potrzeb szkoleniowych uczestników - pretest,

• Dane medyczne i osobowe— kontekst i ryzyka przetwarzanie,

• Zasady postępowania z danymi szczególnie wrażliwymi,

• Zgłaszanie incydentów dot. wycieku danych medycznych i osobowych,

• Przykłady ataków hakerskich na szpitale i placówki ochrony zdrowia,

• Czym jest cyberbezpieczeństwo,

• Metody nieautoryzowanego pozyskania danych wraz z przykładami,

• Zagrożenia w sieci (w tym phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, atak odwrócony - zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa) wraz z przykładami,

• Bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, oraz wewnętrzna bezpieczna komunikacja,

• Bezpieczne hasła, managery haseł, autoryzacja dwuetapowa, klucze sprzętowe,

• Metody obrony oraz przeciwdziałania w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, programowaniem mogącym zablokować dostęp do urządzeń firmowych, szkodliwymi programami mogącymi pozyskać dane firmowe lub osobiste,

• Bezpieczne korzystanie z mediów społecznościowych,

• Bezpieczne korzystanie ze smartfonów,

• Wskazanie miejsc organizacji, oraz informacji, które należy chronić, by zniwelować ryzyko narażenia firmy na straty finansowe,

• Wskazanie zasad cyberhigieny,

• Ewaluacja szkolenia - posttest.

W ramach szkolenia zostaną zorganizowane konsultacje z kadrą zarządzającą. Tematem dyskusji będzie kontekst cyberbezpieczeństwa i prewencji w jednostkach ochrony zdrowia oraz tematyka zarządzania zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).

Minimalny czas trwania szkolenia i konsultacji 3 dni. Szkolenie przewidziane dla liczby minimum 30 uczestników. Szkolenie powinno zostać zrealizowane w formie stacjonarnej lub w szczególnym przypadku (np. wystąpienie uwarunkowań epidemiologicznych) w formie online za wcześniejszą zgodą Zamawiającego.

**4. Skany podatności**

Wykonanie testów podatności infrastruktury teleinformatycznej wraz z przygotowaniem raportu z opisem podatności i rekomendacjami.

W ramach przyszłej realizacji Przedmiotu Umowy zostaną wykonane następujące badania bezpieczeństwa, zgodnie z poniższym opisem

- Identyfikacja i analiza podatności systemów wspomagających świadczenie usługi kluczowej.

Wynikiem analizy musi być pełna lista przeskanowanych pod kątem podatności, systemów zawierająca informacje obejmujące: skanowany system operacyjny, uruchomione na nim usługi, otwarte porty komunikacyjne, listę wykrytych podatności oraz wytyczne dotyczące sposobu usunięcia wykrytych podatności. W celu wykonania powyższych czynności, Wykonawca zobowiązany jest do zapewnienia odpowiedniej licencji na system skanujący. W przypadku tego typu badania nie występuje próba wykorzystania wykrytych podatności, w celu uzyskania dostępu do testowanych systemów.

Usługa powinna zostać zrealizowana zgodnie z Zarządzeniem Prezesa NFZ z 20 maja. Wykonanie usługi skanów podatności, w zakresie sprecyzowanym w materiale referencyjnym „Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia”, opublikowanym na stronie internetowej Centrum e-

Zdrowia3), przez okres do dnia 31 grudnia 2022 r.;

Usługa skanów podatności powinna:

- obejmować przeprowadzenie minimum jednego skanu miesięcznie, przez cały okres obowiązywania Usługi,

- po każdym przeprowadzonym skanie podatności powinien zostać sporządzony i przekazany Zamawiającemu raport z opisem podatności i rekomendacjami,

- usługa powinna zostać dostarczona w formie licencji na okres 36 miesięcy z możliwością opłacenia całego okresu „z góry”,

- Wykonawca powinien zapewnić odpowiednią licencję na system skanujący.

Minimalne wymaganie dla zastosowanego systemu monitorowania:

a. Automatyzacja analizy zdarzeń w systemach operacyjnych Microsoft pod kątem identyfikowania zagrożeń i incydentów bezpieczeństwa IT – system musi rozpoznawać zagrożenia wynikające z niestosowania dobrych praktyk w obszarze zarządzania kontami uprzywilejowanymi (np. zagrożenie ujawnienia hasła zapisanego w pliku tekstowym) oraz w zakresie praktyk stosowanych przez użytkowników (np. zagrożenie wykorzystania konta imiennego przez wielu pracowników).

b. System musi zapewniać ochronę użytkownika poprzez blokowanie komunikacji z źródłami zagrożeń wskazanymi przez platformę N6 CERT Polska.

c. System musi umożliwiać zarządzanie podatnościami informatycznymi. Zarządzanie należy interpretować jako funkcjonalność systemu zadaniowego, w którym to menager może wybierać i przypisywać do realizacji operatorom podatności do usunięcia. System powinien także automatyzować tworzenie zadań, jeśli nie zostanie to zrobione w sposób manualny.

d. System powinien analizować pełen kontekst procesu zarządzania bezpieczeństwem IT i w zależności od roli w organizacji, odpowiednio transformować i prezentować informacje odbiorcy. Jako minimum, role w systemie powinny być dwie: 1) Administrator usług IT, dla którego prezentowane są informacje techniczne, umożliwiające reagowanie i usuwanie zagrożenia w środowisku IT; 2) Właściciel Biznesowy usług IT w organizacji (Zarząd), dla którego prezentowane są informacje zarządcze, np. o efektywności procesu zarządzania bezpieczeństwem IT.

e. Samodzielna ocena dojrzałości organizacyjnej w zakresie zarządzania bezpieczeństwem IT. System musi umożliwiać wykonanie samodzielnego audytu w celu identyfikacji słabości organizacyjnych oraz procesowych w odniesieniu do stosowanych w tym zakresie rynkowych praktyk.

f. System musi umożliwiać wybór standardu, normy bądź innego wymogu formalno-prawnego, wobec którego będzie dokonywał oceny zgodności organizacyjnej.

g. System musi umożliwiać tworzenie własnego zakresu audytu, np. na potrzebę weryfikowania zgodności dostawców, z którymi organizacja ma podpisaną umowę.

h. System musi proponować rekomendacje do wskazanych nieprawidłowości.

i. System musi umożliwiać nadzór nad wdrażaniem działań naprawczych do zaobserwowanych nieprawidłowości.

j. System musi posiadać mechanizm tworzenia raportów czytelnie wskazujących jakie obszary były audytowane, jakie rekomendacje zostały wskazane oraz jaki jest status prac nad ich wdrożeniem.

k. System musi umożliwiać bezpieczną autoryzację użytkownika poprzez wieloskładnikowe uwierzytelnianie (bądź zapewnić możliwość integracji z zewnętrznymi systemami autoryzacji MFA).

Integracje:

a. System musi zapewniać stały dostęp do informacji o zagrożeniach w polskiej sieci Internet publikowanych poprzez z integrację z platformą N6 CERT Polska.

b. System musi posiadać moduł alarmowania o wybranych incydentach oraz zagrożeniach bezpieczeństwa IT. System powinien posiadać możliwość integracji z wybranymi operatorami bramek sms.

Pozostałe:

a. System musi być utworzony i rozwijany przez firmę polską.

1. **Ramowy harmonogram wykonania usługi:**

Realizacja zadań powinna nastąpić w nieprzekraczalnym terminie do dnia 20 listopada 2022 r, w tym:

* Spotkanie koordynacyjne Stron i szczegółowe zaplanowanie realizacji usługi - do 7 dni roboczych od dnia zawarcia Umowy,
* Zadanie1: Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji - do10 listopada 2022 roku,
* Zadanie 2: Przeprowadzenie audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego po wdrożeniu przez Zamawiającego czynności podnoszących poziom bezpieczeństwa systemów teleinformatycznych - do 7 dni roboczych od dnia powiadomienia przez Zamawiającego Wykonawcy o gotowości do poddania się Audytowi. Powiadomienie Wykonawcy przez Zamawiającego o gotowości do poddania się Audytowi powinno nastąpić nie później niż do dnia 10 listopada 2022 r.

Sporządzenie Raportu z Audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego i przekazanie go Zamawiającemu - do 7 dni roboczych od dnia zakończenia Audytu.

* Zadanie 3: Przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa, zgodnie ze szczegółowym zakresem określonym w załączniku do Umowy, w terminie do 21 dni od dnia zawarcia Umowy.
* Zadanie 4: Wykonanie testów podatności infrastruktury teleinformatycznej wraz z przygotowaniem raportu z opisem podatności i rekomendacjami w terminie 21 dni od dnia zawarcia Umowy.

1. **Dodatkowe wymagania:**

Wymagania dla wykonawcy

1) Posiadanie certyfikatów ISO/IEC 27001:2013 oraz ISO 9001:2015

Wymagania dla audytorów (co najmniej dwóch audytorów)

1) Posiadanie certyfikatu audytora wiodącego systemu zarządzania bezpieczeństwem informacji

według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną

zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku

(t.j. Dz. U. z 2021 r. poz. 514 z późn. zm.), w zakresie certyfikacji osób.

2) Posiadanie certyfikatu audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO

22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z

dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz.U. z 2021 r., poz. 514

z późn. zm.), w zakresie certyfikacji osób, lub równoważny.

3) Posiadanie co najmniej trzyletniej praktyki w zakresie audytu bezpieczeństwa systemów

informacyjnych, lub co najmniej dwuletniej praktyki w zakresie audytu bezpieczeństwa systemów

informacyjnych i legitymowanie się dyplomem ukończenia studiów podyplomowych w zakresie

audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w

dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia

naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

4) Za praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, uważa s ię

udokumentowane wykonanie w ciągu ostatnich 3 lat przed dniem rozpoczęcia audytu 3 audytów

w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo wykonywanie

audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania w wymiarze czasu pracy

nie mniejszym niż 1/2 etatu, związanych z:

- przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;

- przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego;

- przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa

w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji

działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r., poz. 2070 z późn.

zm •);

wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 15 lipca 2011 r.

o kontroli w administracji rządowej (t.j. Dz. U. z 2020 r., poz. 224 z późn. zm.);

wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r.

o Najwyższej Izbie Kontroli (t.j. Dz. U. z 2020 r. poz. 1200 z późn. zm.).

5) Wykonanie w okresie ostatnich 3 lat przed upływem terminu składania ofert co najmniej 2 usług polegających na opracowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości działania, w skład którego wchodzi kompletna dokumentacja Bezpieczeństwa Systemu Informacji i Ciągłości działania; o wartości nie mniejszej niż 40 000 PLN netto, w tym jedna usługa zrealizowana była na rzecz podmiotu administracji publicznej.

6) Wykonanie w okresie ostatnich 3 lat przed upływem terminu składania ofert, co najmniej 2 usług polegających na opracowaniu dokumentacji bezpieczeństwa informacji i ciągłości działania, w tym postępowania w sytuacjach kryzysowych w organizacji zatrudniającej nie mniej niż 150 osób.

7) Spełnienie wymagania określonych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018

r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r., poz.

1999).

8) Zamawiający zastrzega prawo wglądu do oryginałów w/w dokumentów oraz dokumentów

potwierdzających zgodność złożonego oświadczenia.

9) Audytorzy są zobowiązani d o zachowania w tajemnicy informacji uzyskanych w związku

z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych

informacji prawnie chronionych.

**Załącznik nr 2  
do umowy …../2022**

**Wykaz osób**

|  |  |  |
| --- | --- | --- |
| **Nazwisko Imię** | **Nr Zadania** | **Kwalifikację zgodnie z ofertą** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Załącznik nr 3**

**Do umowy nr …… /2022**

**WZÓR OŚWIADCZENIA O ZACHOWANIU POUFNOŚCI INFORMACJI**

Ja niżej podpisany/a niniejszym oświadczam, że:

1. nie ujawnię bez stosownego upoważnienia wydanego przez Samodzielny Publiczny Zakład Opieki Zdrowotnej w Łukowie żadnych informacji, w szczególności prawnie chronionych, a także o sposobach zabezpieczenia stosowanych w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Łukowie, o ile wejdę w ich posiadanie, oraz nie przyczynię się do ich ujawnienia lub innych działań związanych z ich przetwarzaniem lub utratą itp. mogących spowodować szkodę dla Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Łukowie, innych osób i podmiotów lub naruszenie przepisów prawa, w tym regulacji Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Łukowie, zarówno w trakcie wykonywania prac w związku z zawartą przez: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ umową \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ jak i po ich zakończeniu oraz będę przestrzegał/a wszelkich przepisów w tym zakresie;
2. zobowiązuję się nie wykraczać poza nadane mi uprawnienia oraz zobowiązuję się wykorzystywać przydzielone mi środki pracy, w tym systemy i urządzenia informatyczne, tylko do celów realizacji ww. umowy;
3. zobowiązuję się przestrzegać oraz jestem świadomy/a odpowiedzialności za naruszenie obowiązujących zasad, wynikających w szczególności z:
   1. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
   2. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| *imię i nazwisko* |  |  | |  | *podpis* |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Miejscowość, data*

**Załącznik nr 4**

**Do umowy nr …… /2022**

**Umowa powierzenia przetwarzania danych**

zwana dalej **„Umową”**,

zawarta dnia…………………………………

pomiędzy:

**Samodzielnym Publicznym Zakładem Opieki Zdrowotnej w Łukowie**, 21 – 400 Łuków, ul. Doktora Andrzeja Rogalińskiego 3, wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej w Sądzie Rejonowym Lublin-Wschód w Lublinie z siedzibą w Świdniku VI Wydziale Gospodarczym Krajowego Rejestru Sądowego, KRS Nr 000056773, REGON: 000306472, NIP: 825 – 17 – 11 – 719zwanym dalej **„Administratorem”**,

reprezentowanym przez **Mariusza Furlepa – Dyrektora SPZOZ w Łukowie**

a

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

zwanym dalej **„Podmiotem przetwarzającym”**,

reprezentowanym przez…………………………………………………………………………………..

zwanymi łącznie **„Stronami”**.

Mając na uwadze, iż Strony łączy umowa……….z dnia…………………………, zwana dalej **„Umową główną”**, w związku z wykonywaniem, której przetwarzane są dane osobowe, Strony zgodnie postanowiły, co następuje:

**§ 1.**

**Powierzenie przetwarzania danych osobowych**

1. Administrator, w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwanego dalej „Rozporządzeniem”, powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia oraz innych przepisów, o których mowa w ust. 2.

**§2.**

**Zakres i cel przetwarzania danych**

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie umowy dane osobowe i dane medyczne pacjentów oraz dane osobowe pracowników.
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy z dnia …… nr ………w zakresiewdrożenia Systemu Zarządzania Bezpieczeństwem Informacji, przeprowadzenia audytu spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa przez operatora usługi kluczowej, przeprowadzenia szkolenia z zakresu cyberbezpieczeństwa oraz wykonania testów podatności infrastruktury teleinformatycznej wraz z przygotowaniem raportu z opisem podatności i rekomendacjami.

**§ 3.**

**Obowiązki podmiotu przetwarzającego**

1. Podmiot przetwarzający zobowiązuje się przy przetwarzaniu powierzonych danych, wskazanych w § 2, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa, odpowiadający ryzyku związanemu   
   z przetwarzaniem danych osobowych, o którym mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy,   
   w tym do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, o której mowa w art. 28 ust. 3 lit. b Rozporządzenia, przetwarzanych danych przez osoby, które upoważnione zostaną do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie trwania zatrudnienia ich u Podmiotu przetwarzającego, jak i po jego ustaniu.
5. Podmiot przetwarzający zobowiązuje się pomagać, w miarę możliwości, Administratorowi w niezbędnym zakresie w wywiązywaniu się przez niego z:
6. obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III Rozporządzenia;
7. obowiązków określonych w art. 32 - 36 Rozporządzenia.
8. Podmiot przetwarzający powiadamia Administratora o każdym podejrzeniu naruszenia ochrony danych osobowych powierzonych Umową, niezwłocznie, nie później niż 24 h od chwili uzyskania informacji   
   o potencjalnym naruszeniu oraz umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności   
   o stwierdzeniu faktycznego naruszenia.

**§ 4.**

**Prawo kontroli**

1. Zgodnie z art. 28 ust. 3 lit. h Rozporządzenia Administrator ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy i Rozporządzenia.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu powierzającego   
   i z minimum 7 dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli,   
   o której mowa w ust. 1, w terminie wskazanym przez Administratora.
4. Podmiot przetwarzający zobowiązuje się do udostępnienia Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia przez siebie obowiązków określonych w art. 28 Rozporządzenia.

**§ 5.**

**Odpowiedzialność Podmiotu przetwarzającego**

1. Podmiot przetwarzający odpowiedzialny jest za przetwarzanie danych osobowych niezgodnie z treścią Umowy, przepisami Rozporządzenia lub innymi przepisami, o których mowa w § 1 ust. 2,   
   a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o wszelkich wiadomych mu:
3. postępowaniach, w szczególności sądowych lub administracyjnych,
4. decyzjach administracyjnych i orzeczeniach sądowych,
5. planowanych lub realizowanych kontrolach i inspekcjach, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych,

dotyczących danych, o których mowa w § 2 Umowy, powierzonych przez Administratora**.**

**§ 6.**

**Podpowierzenie**

1. Podmiot przetwarzający może powierzyć dane osobowe, wskazane w § 2 Umowy**,**  do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy oraz po uzyskaniu uprzedniej zgody Administratora. Zgoda Administratora musi mieć formę pisemną pod rygorem nieważności.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora, chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w ust. 1, winien spełniać te same wymogi i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie, w szczególności w zakresie gwarancji ochrony powierzonych danych osobowych.
4. Podmiot przetwarzający ponosi wobec Administratora pełną odpowiedzialność za niewywiązywanie się przez podwykonawcę ze spoczywających na nim obowiązków ochrony danych.

**§ 7.**

**Zasady zachowania poufności**

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych w związku z realizacją Umowy od Administratora i współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały ich zabezpieczenie, w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

**§ 8.**

**Czas obowiązywania umowy**

1. Umowa zostaje zawarta na czas trwania Umowy głównej. W celu uniknięcia wątpliwości, rozwiązanie Umowy głównej skutkuje rozwiązaniem niniejszej Umowy.
2. Strony postanawiają, iż po zakończeniu przetwarzania danych Podmiot przetwarzający zobowiązany jest do niezwłocznego usunięcia powierzonych mu danych (i wszelkich ich istniejących kopii) lub zwrotu Administratorowi – w zależności od jego decyzji, i ile nie następuje konieczność dalszego przetwarzania danych wynikająca z przepisów odrębnych.

**§ 9.**

**Wypowiedzenie umowy**

Administrator uprawniony jest do rozwiązania Umowy bez wypowiedzenia, jeżeli Podmiot przetwarzający nie podjął środków zabezpieczających powierzone dane lub nie stosował się do wymogów przewidzianych w Rozporządzeniu, w tym:

1. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
2. przetwarza dane osobowe w sposób niezgodny z umową,
3. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

**§ 10.**

**Postanowienia końcowe**

1. Każda ze stron odpowiada za szkody wyrządzone drugiej stronie oraz osobom trzecim w związku z wykonywaniem niniejszej Umowy, zgodnie z przepisami Rozporządzenia i Kodeksu cywilnego.
2. W celu uniknięcia wątpliwości, Podmiot przetwarzający ponosi odpowiedzialność za działania swoich pracowników i innych osób, przy pomocy, których przetwarza powierzone dane osobowe, jak za własne działanie i zaniechanie.
3. W sprawach nieuregulowanych niniejszą Umową zastosowanie mają powszechnie obowiązujące przepisy prawa polskiego.
4. Wszelkie zmiany lub uzupełnienia niniejszej Umowy wymagają zachowania formy pisemnej pod rygorem nieważności.
5. Sądem właściwym dla rozstrzygania sporów powstałych w związku z realizacją niniejszej Umowy jest sąd właściwy dla siedziby Administratora.
6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
7. Umowa wchodzi w życie z dniem podpisania.

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

**Administrator Podmiot przetwarzający**