**SZCZEGÓŁOWE**

**WYMAGANIA W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH**

1. Umowa Nr …………….…………... na usługę polegającej na realizacji w formie całodobowej stałej i bezpośredniej ochrony fizycznej osób, mienia, terenów, obiektów, urządzeń w systemie zmianowym w dni robocze, świąteczne i wolne od pracy, realizowanej z wykorzystaniem kwalifikowanych pracowników ochrony fizycznej Specjalistycznej Uzbrojonej Formacji Ochronnej (SUFO), monitorowaniu alarmów z wykorzystaniem oddalonych centrów monitorowania, stałym dozorze sygnałów przesyłanych, gromadzonych i przetwarzanych w elektronicznych urządzeniach i systemach alarmowych, patrolowaniu obiektów oraz utrzymania porządku publicznego w kompleksach wojskowych jednostek i instytucji wojskowych będących na zaopatrzeniu 32 Wojskowego Oddziału Gospodarczego w Zamościu wiąże się z dostępem do informacji niejawnych o klauzuli **ZASTRZEŻONE**.
2. **W celu zapewnienia właściwej ochrony informacji niejawnych dotyczących przedmiotu umowy Wykonawca zobowiązany jest do przestrzegania zasad ochrony informacji niejawnych zawartych** w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2025.1209 t.j.) oraz wydanych na jej podstawie przepisach wykonawczych.
3. **W niniejszym dokumencie używa się następujących określeń:**
4. **Ustawa** - ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2025.1209 t.j.)
5. Zamawiający  **32 Wojskowy Oddział Gospodarczy w Zamościu**
6. Wykonawca zgodnie z podpisaną umową nr ……….……………
7. Użytkownik (kompleksu, obiektu): 32 Wojskowy Oddział Gospodarczy.
8. Wykonawca, pod rygorem zerwania umowy z winy Wykonawcy i odpowiedzialności karnej za ujawnienie informacji niejawnych udostępnionych przez Zamawiającego lub Użytkownika, bądź wytworzonych w trakcie realizacji przedmiotu umowy, zobowiązany jest do przestrzegania i stosowania przepisów i procedur właściwych do ochrony informacji niejawnych zgodnie z **Ustawą**.
9. Ochronie podlegają informacje niejawne o klauzuli **ZASTRZEŻONE** oraz informacje związane z realizacją umowy dotyczące:
10. miejsca i zakresu wykonywanych prac, funkcjonowania systemu ochrony obiektu, prowadzonych rozmów stron umowy;
11. przeznaczenia budynków i urządzeń w obiekcie Zamawiającego i Użytkowników;
12. informacji dotyczących Użytkownika obiektu;
13. innych informacji związanych z bezpieczeństwem obiektu uzyskanych w związku z realizacja umowy;
14. pozostałych materiałów określonych w art. 2 pkt. 4 **Ustawy**;
15. wszelkie materiały otrzymane od Zamawiającego do zapoznania się w siedzibie Zamawiającego lub otrzymane do opracowania w siedzibie Wykonawcy.
16. Wykonawca umowy jest zobowiązany posiadać:

* Kierownik przedsiębiorcy w rozumieniu ustawy winien posiadać co najmniej szkolenie w zakresie ochrony informacji niejawnych wydane na podstawie art.19 Ustawy (Podstawa: art. 54 **Ustawy**.)
* Pełnomocnika ochrony przeszkolonego w zakresie ochrony informacji niejawnych przez ABW lub SKW;
* Wykonawca winien wykazać zdolność do przetwarzania informacji niejawnych o klauzuli „ZASTRZEŻONE” zgodnie z art. 43 ust. 5 UOIN, tj. posiadać instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o tej klauzuli oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.
* Wykonawca winien dysponować systemem teleinformatycznym umożliwiającym przetwarzanie informacji niejawnych o klauzuli „ZASTRZEŻONE” akredytowanym zgodnie z wymogami **Ustawy**.
* Pracownicy przewidziani do realizacji przedmiotu umowy winni posiadać poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych lub pisemne upoważnienie wydane na podstawie art. 21 ust.4 pkt.1 ustawy wraz z zaświadczeniem o odbyciu szkolenia w zakresie ochrony informacji niejawnych.

1. Wymagane dokumenty potwierdzające uprawnienia w zakresie ochrony informacji niejawnych:
2. Kierownik przedsiębiorcy:

* zaświadczenie o odbyciu szkolenia w zakresie ochrony informacji niejawnych zgodnie z art. 19, art. 20 ust. 1, w związku z art. 2 ust. 14 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2025.1209 t.j.) – dalej UOIN,

1. Pełnomocnik ds. Ochrony Informacji Niejawnych:

* zaświadczenie o odbyciu szkolenia w zakresie ochrony informacji niejawnych zgodnie z art. 14 ust. 3 pkt 4 UOIN,
* poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych zgodnie z art. 22 ust.2, w związku z art. 14 ust. 2 UOIN,

1. Inspektor Bezpieczeństwa Teleinformatycznego:

* zaświadczenie o odbyciu szkolenia w zakresie ochrony informacji niejawnych zgodnie z art. 19, art. 20 ust. 1 UOIN,
* poświadczenie bezpieczeństwa lub pisemne upoważnienie kierownika jednostki organizacyjnej do dostępu do informacji niejawnych o klauzuli „ZASTRZEŻONE” zgodnie z art. 21 ust.4, w związku z art. 52 ust. 1 pkt 1 UOIN,
* zaświadczenie o odbyciu szkolenia specjalistycznego w zakresie bezpieczeństwa teleinformatycznego zgodnie z art. 52 ust. 4, w związku z art. 52 ust. 1 pkt 1 UOIN,

1. Administrator Systemu:

* zaświadczenie o odbyciu szkolenia w zakresie ochrony informacji niejawnych zgodnie z art. 19, art. 20 ust. 1 UOIN,
* poświadczenie bezpieczeństwa lub pisemne upoważnienie kierownika jednostki organizacyjnej do dostępu do informacji niejawnych o klauzuli „ZASTRZEŻONE” zgodnie z art. 21 ust.4, w związku z art. 52 ust. 1 pkt 2 UOIN,
* zaświadczenia o odbyciu szkolenia specjalistycznego w zakresie bezpieczeństwa teleinformatycznego zgodnie z art. 52 ust. 4, w związku z art. 52 ust. 1 pkt 2 UOIN.

1. Inne osoby biorące udział w realizacji przedmiotu zamówienia:

* zaświadczenie o odbyciu szkolenia w zakresie ochrony informacji niejawnych zgodnie z art. 19, art. 20 ust. 1 UOIN,
* poświadczenie bezpieczeństwa lub pisemne upoważnienia kierownika jednostki organizacyjnej do dostępu do informacji niejawnych o klauzuli „ZASTRZEŻONE” zgodnie z art. 21 ust.4 UOIN,

1. Kserokopia pierwszej strony instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli „ZASTRZEŻONE” w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony, opracowanej zgodnie z art. 43 ust. 5 UOIN.
2. Kserokopia świadectwa bezpieczeństwa przemysłowego pierwszego stopnia,

**lub**

kserokopia świadectwa akredytacji systemu teleinformatycznego dla klauzuli innej niż „ZASTRZEŻONE”,

**lub**

kserokopia ze stron dokumentacji bezpieczeństwa systemu teleinformatycznego zawierającą informacje o zatwierdzeniu tej dokumentacji przez kierownika jednostki organizacyjnej w przypadku systemu do przetwarzania informacji niejawnych o klauzuli „ZASTRZEŻONE” (Procedury Bezpiecznej Eksploatacji i Szczególne Wymagania Bezpieczeństwa) wraz z kserokopią pisma ABW/SKW potwierdzającego, że opracowana w/w dokumentacja systemu (PBE i SWB) spełnia wymogi formalne zawarte w UOIN oraz rozporządzeniach w zakresie eksploatacji systemu lub oświadczeniem kierownika jednostki organizacyjnej o udzieleniu akredytacji dla systemu teleinformatycznego o klauzuli „ZASTRZEŻONE”,

1. **(jeżeli dotyczy)** Kserokopia porozumienia między kierownikami jednostek organizacyjnych w zakresie dysponowania systemem teleinformatycznym akredytowanym do przetwarzania informacji o klauzuli co najmniej „ZASTRZEŻONE” udostępnionym przez inną jednostkę,
2. **(jeżeli dotyczy)** Kserokopia zgody ABW lub SKW na wykonywanie zadań przez administratora systemu teleinformatycznego lub inspektora bezpieczeństwa teleinformatycznego w innej jednostce organizacyjnej wraz z kserokopią porozumienia w ww. kwestii między kierownikami jednostek organizacyjnych,
3. W przypadku realizacji zadania przez konsorcjum firm, wszystkie osoby przewidziane do realizacji zadania winny posiadać uprawnienia w zakresie bezpieczeństwa osobowego określone w UOIN,
4. Umowa konsorcjum winna w sposób jednoznaczny regulować zadania poszczególnych członków w zakresie przetwarzania informacji niejawnych, z uwzględnieniem przetwarzania informacji niejawnych w systemach teleinformatycznych.
5. Wykonawca potwierdza spełnienie warunków określonych w niniejszych „Szczególnych wymaganiach w zakresie ochrony informacji niejawnych” dokumentami złożonymi w postepowaniu przetargowym. W przypadku realizacji zadania przez konsorcjum firm, lider konsorcjum musi wskazać   
   w umowie konsorcjum, Wykonawcę odpowiedzialnego za bezpieczeństwo przetwarzania informacji niejawnych.
6. Wykonawca w trakcie trwania umowy – bez pisemnej zgody Zamawiającego – nie może powierzyć ani cedować swoich uprawnień wynikających z umowy lub jej części innym osobom lub firmom.
7. W przypadku podpisania umowy z Podwykonawcą, Podwykonawca przed przystąpieniem do realizacji umowy potwierdza spełnienie warunków określonych w niniejszych „Szczególnych wymaganiach w zakresie ochrony informacji niejawnych” składając Zamawiającemu stosowne oświadczenie oraz zobowiązany jest realizować przedmiot umowy zgodnie z warunkami stawianymi Wykonawcy.
8. W przypadku utraty ważności Świadectwa Bezpieczeństwa Przemysłowego lub Akredytacji Systemu Teleinformatycznego Wykonawca zobowiązany jest bezzwłocznie do przesłania Zamawiającemu kserokopii przedmiotowych dokumentów potwierdzonych za zgodność z oryginałem.
9. Wykonawca zobowiązany jest przekazać Zamawiającemu aktualny „Wykaz osób przewidzianych do realizacji przedmiotu umowy", (wg wzoru stanowiącego załącznik do OPZ/SWZ) wraz z poświadczonymi za zgodność z oryginałem dokumentami wymienionymi w pkt. 6, oraz bezzwłocznej aktualizacji powyższych dokumentów w przypadku utraty ich ważności.
10. Wykonawca powiadomi Zamawiającego pisemnie o zamiarze wprowadzenia nowych pracowników, z co najmniej pięciodniowym wyprzedzeniem lub natychmiast w nagłych przypadkach, załączając do powiadomienia potwierdzone za zgodność kserokopie: legitymacji kwalifikowanego pracownika zabezpieczenia technicznego, legitymacji pracownika ochrony fizycznej, poświadczenia bezpieczeństwa osobowego lub pisemnego upoważnienia wydanego na podstawie art. 21 ust.4 pkt.1 ustawy oraz zaświadczenia o odbyciu szkolenia w zakresie ochrony informacji niejawnych.
11. Pracownicy skierowani do realizacji zamówienia zobowiązani są wykonywać swoją pracę samodzielnie, bez uprawnienia do wprowadzania w ramach zastępstwa do ochranianego obiektu osób trzecich.
12. Wymagania w zakresie zabezpieczenia informacji i materiałów podczas realizacji umowy:
13. Prace związane z dostępem do informacji niejawnych realizowane w siedzibie Wykonawcy, winny być prowadzone w oparciu o instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „Zastrzeżone” oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony, opracowaną zgodnie z art. 43 ust. 5 UOIN,
14. Systemy teleinformatyczne Wykonawcy wykorzystywane do prac związanych z wykonaniem zadań wynikających z przedmiotu umowy muszą spełniać wymagania określone w :
15. ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (rozdział 8: bezpieczeństwo teleinformatyczne),
16. rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań w zakresie bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r. nr 159 poz. 948);
17. rozporządzeniu Rady Ministrów z dnia 29 maja 2012r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. z 2012 r. poz.683 z późn. zm.).
18. Oznaczenia wykonanych materiałów należy dokonać zgodnie  
    z rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r.   
    w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. z 2011 r. nr 288 poz.1692).
19. Sporządzenie kopii materiału niejawnego może nastąpić za pisemną zgodą Zamawiającego. Sporządzone kopie podlegają ewidencji na zasadach określonych w rozporządzeniu Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. z 2011 r. nr 288 poz.1692).
20. Wszystkie przekazane materiały przez Wykonawcę po ich wykorzystaniu muszą być niezwłocznie zwrócone Zamawiającemu (*Dowódcy JW na rzecz której realizowana jest usługa),* jednak nie później niż w dniu zakończenia umowy albo niezwłocznie w przypadku odstąpienia od umowy przez którąkolwiek ze stron. Do wydawania i przyjmowania materiałów niejawnych w imieniu Zamawiającego upoważniony jest personel Kancelarii Tajnej Zamawiającego. Niszczenie materiałów niejawnych przekazanych przez Zamawiającego jest zabronione.
21. Po zakończeniu realizacji przedmiotu zamówienia lub odstąpienia od umowy przez którąkolwiek ze stron, dane zawarte w systemach teleinformatycznych dotyczące Zamawiającego muszą być bezwzględnie w sposób trwały usunięte z informatycznych nośników danych (IND) Wykonawcy. Wykonawca złoży pisemne oświadczenie Zamawiającemu o realizacji powyższego obowiązku, nie później niż w dniu zakończenia umowy albo niezwłocznie w przypadku odstąpienia od umowy przez którąkolwiek ze stron.
22. Wymiana korespondencji niejawnej pomiędzy stronami umowy odbywać się musi zgodnie z zasadami zawartymi w:
23. ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,
24. rozporządzeniu Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. z 2017 r. poz. 1558 t.j.),
25. zarządzeniu Nr 58/MON z dnia 11 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu   
    i trybu przetwarzania informacji niejawnych (Dz. Urz. MON z 2017 r. poz. 226 z późn. zm.),
26. rozporządzeniu Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów niejawnych zawierających informacje niejawne (Dz.U. z 2011 r. nr 271 poz. 1603).
27. Zabrania się posługiwania wszelkimi nieoznaczonymi informatycznymi nośnikami danych (IND) w systemach lub sieciach teleinformatycznych Wykonawcy w ramach realizacji umowy.
28. Wymagania w zakresie zabezpieczenia miejsca przechowywania  
    i przetwarzania materiałów niejawnych związanych z przedmiotem umowy:
29. Materiały niejawne przekazane Wykonawcy przetwarzać zgodnie

z zapisami w:

1. rozporządzeniu Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. z 2017 r. poz. 1558 t.j.),
2. rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. z 2012 r. poz. 683 z późn. zm.).
3. Wykonawca zobowiązany jest do zachowania poufnego charakteru informacji niejawnych, z którymi zapozna się w trakcie realizacji zamówienia i po jego zakończeniu.
4. Przedmiot umowy, wszelkie informacje oraz materiały uzyskane w czasie   
   i po jego realizacji nie mogą być wykorzystane do żadnego rodzaju materiałów promocyjnych i czynności z tym związanych, w szczególności prezentacji w środkach masowego przekazu, filmach, ulotkach, folderach itp.
5. W przypadku naruszenia zasad bezpieczeństwa obiektu podlegającego ochronie, Wykonawca podejmie niezwłoczne działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków oraz powiadomi o powyższym fakcie kierownika jednostki organizacyjnej Zamawiającego i Użytkownika.
6. W przypadku stwierdzenia przez Zamawiającego naruszenia przez pracownika Wykonawcy podczas realizacji umowy przepisów Ustawy lub niniejszych postanowień, Zamawiający zastrzega prawo do złożenia wniosku o wykluczenie go z dalszej realizacji umowy, a w uzasadnionych przypadkach również podjęcia kroków dotyczących odpowiedzialności karnej pracownika.
7. Wykonawca ponosi pełną odpowiedzialność za należyte wykonanie usług oraz wszelkie szkody spowodowane nieprawidłowym wykonaniem obowiązków przez swoich pracowników oraz powierzonych Podwykonawcy.
8. W procesie opracowywania umów związanych z dostępem do informacji niejawnych zapewniono uczestnictwo pełnomocników ochrony jednostek organizacyjnych, na rzecz których realizowana jest umowa.
9. Za zapewnienie warunków ochrony informacji niejawnych z ramienia Wykonawcy odpowiedzialny jest ………..……………………………………… tel.:…………………
10. Z ramienia Zamawiającego i Użytkownika za bieżącą kontrolę bezpieczeństwa przedmiotu ochrony, nadzór oraz doradztwo w zakresie wykonywania przez Wykonawcę obowiązku ochrony udostępnianych informacji niejawnych jest:
11. Z ramienia Zamawiającego: p. Robert Kłak, tel. 261 181 529
12. Z ramienia Użytkownika: ……………………………………..

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **WYKONAWCA** | |  | **ZAMAWIAJĄCY** | |
| PEŁNOMOCNIK ds. OIN  WYKONAWCY | |  | PEŁNOMOCNIK ds. OIN  ZAMAWIAJĄCEGO | |
|  | |  |  | |
|  | |  |  | |
|  | **UŻYTKOWNIK** | | |  |
|  | PEŁNOMOCNIK ds. OIN  UŻYTKOWNIKA | | |  |
|  |  | | |  |

Robert Kłak tel. 261181529

03.11.2025 r.

T – 2712 B5