ISTOTNE POSTANOWIENIA UMOWY

**§ 1**

**Przedmiot Umowy**

1. W ramach Umowy Wykonawca w przypadku zaoferowania innego rozwiązania niż obecnie eksploatowanego przez Zamawiającego zobowiązuje się na rzecz Zamawiającego do:
	1. udzielenia lub zapewnienia udzielenia niewyłącznych licencji dla Zamawiającego, na czas nieoznaczony, od daty udostępnienia licencji przez Wykonawcę, na terytorium całego świata, na oprogramowanie do zarządzania informacją i zdarzeniami bezpieczeństwa, zwanego w dalszej części umowy „oprogramowaniem” lub „Systemem”:

………………………………………………………………………………………………………………………..…. *(zostanie wpisana nazwa oprogramowania zgodnie z ofertą Wykonawcy)*;

* 1. wykonania wdrożenia oprogramowania na serwerach Ministerstwa Sprawiedliwości w siedzibie Zamawiającego przy ul. Czerniakowskiej 100 w Warszawie. Na wniosek Wykonawcy Zamawiający może wyrazić zgodę w formie pisemnej na wykonanie prac zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Zamawiającego;
	2. udzielenia gwarancjina oprogramowanie, przez okres 12 miesięcy licząc od daty podpisania przez Zamawiającego bez zastrzeżeń protokołu odbioru wdrożonego
	Systemu, zgodnie z załącznikiem 2b;
	3. przeprowadzenia instruktażu stanowiskowego dla pracowników Zamawiającego (do 6 administratorów) w zakresie działań administracyjnych dla oprogramowania ;
	4. opracowania i dostarczenia projektu technicznego i dokumentacji powykonawczej,
	5. zapewnienia asysty Wykonawcy przez okres trwania umowy w wymiarze do 320 roboczogodzin, polegającego na świadczeniu usług konfiguracji, modernizacji, optymalizacji dla oprogramowania.
1. W przypadku zaoferowania rozwiązania już eksploatowanego przez Zamawiającego opisanego w Załączniku nr 1:
	1. udzielenia lub zapewnienia udzielenia niewyłącznych licencji dla Zamawiającego, na okres od 20.10.2021 do 20.10.2022, na terytorium całego świata, na oprogramowanie do zarządzania informacją i zdarzeniami bezpieczeństwa, zwanego w dalszej części umowy „oprogramowaniem” lub „Systemem”
	2. udzielenia gwarancji, na oprogramowanie, przez okres od 20.10.2021 do 20.10.2022.
2. Szczegółowy Opis Przedmiotu Umowy zawiera Załącznik nr 1 do Umowy.
3. Miejscem realizacji Umowy jest siedziba Zamawiającego: ul. Czerniakowska 100, 00-454 Warszawa. Zamawiający wskaże Wykonawcy miejsce wdrożenia Systemu.

**§ 2**

**Termin i sposób realizacji Umowy**

1. W przypadku zaoferowania rozwiązania innego niż obecnie eksploatowanego przez Zamawiającego w terminie **do 5 dni roboczych** od dnia zawarcia umowy Strony uzgodnią wymagania niezbędne do przygotowania przez Zamawiającego infrastruktury pod wdrożenie Systemu.
2. Dla potwierdzenia praw do korzystania przez Zamawiającego z Systemu, Wykonawca dostarczy Zamawiającemu dokumenty licencyjne na indywidualne konto kontaktu technicznego wskazanego przez Zamawiającego, zarejestrowanych na rzecz Ministerstwa Sprawiedliwości, Al. Ujazdowskie 11, 00-950 Warszawa, w terminie do **14 dni kalendarzowych** od dnia zawarcia umowy.
3. W przypadku zaoferowania rozwiązania innego niż obecnie eksploatowanego przez Zamawiającego Wykonawca zobowiązany jest dokonać wdrożenia Systemu, przeprowadzić instruktaż stanowiskowy oraz wykonać dokumentację powykonawczą w terminie do **20** **października 2021 r.**, pod warunkiem udostępnienia przez Zamawiającego poprawnie skonfigurowanej infrastruktury pod wdrożenie Systemu.
4. W przypadku zaoferowania rozwiązania innego niż obecnie eksploatowanego przez Zamawiającego, Zamawiający w terminie 2 dni roboczych od otrzymania dokumentacji powykonawczej dokonuje jej akceptacji lub zgłasza do niej uwagi, przesyłając je na adres poczty elektronicznej….
5. W przypadku zaoferowania rozwiązania innego niż obecnie eksploatowanego przez Zamawiającego Wykonawca zobowiązany jest w terminie 2 dni roboczych od dnia otrzymania uwag do ich uwzględniania i przedstawienia poprawionej wersji dokumentacji powykonawczej, a w razie nieuwzględnienia uwag – do pisemnego uzasadnienia swojego stanowiska.
6. Przekazanie dokumentów licencyjnych zostanie potwierdzona protokołem odbioru podpisanym przez przedstawiciela Zamawiającego w ciągu 3 dni roboczych od daty ich dostarczenia. Wzór protokołu odbioru licencji stanowi **Załącznik nr 2a** do Umowy.
7. W przypadku zaoferowania rozwiązania innego niż obecnie eksploatowanego przez Zamawiającego, wykonanie wdrożenia, przeprowadzenie instruktażu stanowiskowego dla pracowników Zamawiającego oraz wykonanie dokumentacji powykonawczej zostanie potwierdzone protokołami odbioru podpisanymi przez Zamawiającego, zgodnie ze wzorem stanowiącym odpowiednio **Załącznik nr 2b, Załączniki nr 2c oraz** **Załączniki nr 2f** do Umowy.
8. W ramach realizacji przedmiotu umowy, o którym mowa w § 1 ust. 1 pkt 6, Zamawiający będzie zlecał wykonywanie prac przesyłając formularz zlecenia, którego wzór stanowi załącznik nr 2d do umowy, na adres email, o którym mowa w § 4 ust. 2.
9. Zakres każdego zlecenia będzie każdorazowo określany przez Zamawiającego w formularzu zlecenia.
10. Wykonawca określa pracochłonność i termin wykonania zlecenia przesyłając Zamawiającemu uzupełniony formularz zlecenia na adres email, o którym mowa w § 4 ust. 1.
11. Zamawiający składa oświadczenie o akceptacji propozycji Wykonawcy albo oświadczenie o odstąpieniu od realizacji zlecenia na warunkach przedstawionych przez Wykonawcę przesyłają je na adres email, o którym mowa w § 4 ust. 2. Wykonawca podejmie realizację zlecenia po akceptacji przez Zamawiającego pracochłonności i terminu wykonania zlecenia zaproponowanych przez Wykonawcę. Wykonawca może realizować zlecenie tylko i wyłącznie w przypadku złożenia oświadczenia Zamawiającego o akceptacji pracochłonności i terminu wykonania zlecenia.
12. Odbiór danego zlecenia będzie następował poprzez sporządzenie protokołu odbioru zlecenia, którego wzór stanowi Załącznik nr 2e do Umowy.
13. Zamawiający w ciągu 3 dni roboczych potwierdzi odebranie wykonanych usług w ramach danego zlecenia i podpisze protokół odbioru albo zgłosi na piśmie uwagi co do wykonania zlecenia. W przypadku zgłoszenia przez Zamawiającego uwag Wykonawca w terminie 3 dni roboczych wykona ponownie zlecenie albo przedstawi wyjaśnienie dotyczące uwag zgłoszonych przez Zamawiającego i ponownie przedkłada do akceptacji protokół odbioru Zamawiającemu. Po ponownym przedłożeniu protokołu odbioru Zamawiającemu do akceptacji, Zamawiający podpisuje protokół albo odmawia jego zaakceptowania. Odmowa akceptacji protokołu wymaga pisemnego uzasadnienia.

**§ 3**

**Wynagrodzenie umowne oraz warunki płatności**

1. Wynagrodzenie należne Wykonawcy za cały okres realizacji umowy nie przekroczy kwoty **……………..**  **zł brutto** (słownie: ……………………… zł), w tym:
2. w zakresie przedmiotu umowy określonego w § 1 ust. 1 pkt 1-5 - ………….. zł (słownie: ………….) brutto,
3. w zakresie przedmiotu umowy określonego w § 1 ust. 1 pkt 6 – ………….. zł (słownie: ………….) brutto za każdą zrealizowaną godzinę wsparcia, tj. łącznie ………………… zł brutto (słownie: ………………).
4. Wynagrodzenie określone w ust. 1 zawiera wszelkie koszty związane z realizacją Umowy, w tym opłaty, podatki i należności wynikające z obowiązujących przepisów prawa, jak również koszt wdrożenia Systemu, wszelkie koszty i wynagrodzenie związane z uzyskaniem licencji na System oraz udzieleniem lub zapewnieniem udzielenia licencji na System, wynagrodzenie i koszty związane z przeprowadzeniem instruktażu stanowiskowego dla pracowników Zamawiającego.
5. W przypadku zaoferowania rozwiązania innego niż obecnie eksploatowanego przez Zamawiającego podstawą do wystawienia faktury w zakresie przedmiotu umowy określonego w § 1 ust. 1 pkt 1-5 umowy będą łącznie, protokoły obioru stanowiące odpowiednio **Załącznik nr 2a, Załącznik nr 2b, Załączniki nr 2c oraz** **Załączniki nr 2f** do Umowy, podpisane przez Zamawiającego bez zastrzeżeń. Wynagrodzenie za wykonanie przedmiotu umowy, o którym mowa w § 1 ust. 1 pkt 6, zostanie obliczone na podstawie faktycznie wykorzystanych roboczogodzin i ceny jednostkowej wskazanej w ust. 2 pkt 2, wskazanych w formularzu zlecenia. Minimalną jednostką rozliczeniową jest godzina zegarowa świadczonych prac. Każdą rozpoczętą godzinę wykonanych prac uznaje się za pełną godzinę zegarową pracy jednego przedstawiciela Wykonawcy.
6. W przypadku zaoferowania rozwiązania obecnie eksploatowanego przez Zamawiającego podstawą do wystawienia faktury, będzie protokół odbioru stanowiący **Załącznik nr 2a,** do Umowy, podpisany przez Zamawiającego bez zastrzeżeń.
7. W przypadku nie wykorzystania przez Zamawiającego całego wynagrodzenia, o którym mowa w ust. 1 pkt 2, Wykonawcy nie przysługują żadne roszczenia z tego tytułu wobec Zamawiającego, w tym roszczenie o zapłatę wynagrodzenia za niezrealizowaną część umowy.
8. Płatność dokonana będzie na podstawie faktury wystawionej na Ministerstwo Sprawiedliwości, Al. Ujazdowskie 11, 00-950 Warszawa, NIP 5261673166, przelewem bankowym z rachunku Zamawiającego na rachunek Wykonawcy wskazany na fakturze, w terminie **21** **dni** od otrzymania prawidłowo wystawionej faktury.
9. Za dzień zapłaty faktury uważa się dzień obciążenia rachunku bankowego Zamawiającego.

**§4**

**Osoby do kontaktu**

1. Ze strony Zamawiającego osobami odpowiedzialnymi za realizację Umowy oraz upoważnionymi do kontaktów i do podpisania protokołów odbioru są:

- ………………………………………. tel. …………………………………., e-mail …………………….

 - ………………………………………. tel. …………………………………., e-mail …………………….

1. Ze strony Wykonawcy osobami odpowiedzialnymi za realizację Umowy oraz upoważnionymi do kontaktów i do podpisywania protokołów odbioru są :

- ………………………………………. tel. …………………………………., e-mail …………………….

- ………………………………………. tel. …………………………………., e-mail …………………….

1. Zmiana osób i danych wskazanych w ust. 1 i 2 nie wymaga zawarcia aneksu do Umowy i dla swej skuteczności wymaga pisemnego powiadomienia drugiej Strony.

**§5**

**Obowiązki Wykonawcy**

1. Wykonawca oświadcza, że posiada wszelkie kwalifikacje, uprawnienia, doświadczenie i środki materialne oraz urządzenia niezbędne do wykonania Umowy.
2. Wykonawca zobowiązuje się do wykonania Przedmiotu Umowy zgodnie z parametrami i wymaganiami określonymi w **Załączniku nr 1** do Umowy.
3. Wykonawca ponosi całkowitą odpowiedzialność za skutki działania lub zaniechania osób, przy udziale których lub z pomocą których realizuje niniejszą Umowę.
4. Wykonawca zobowiązany jest wykonać Umowę z zachowaniem najwyższej staranności wymaganej od czołowych przedsiębiorców świadczących na terytorium Rzeczypospolitej Polskiej usługi informatyczne.
5. Wykonawca ponosi całkowitą odpowiedzialność za własne działania lub zaniechania, związane z realizacją Umowy, chyba że szkoda nastąpiła wskutek siły wyższej albo wyłącznie z winy Zamawiającego lub osoby trzeciej.
6. Wykonawca, z chwilą podpisania protokołu odbioru w zakresie wdrożenia określonego w § 1 ust. 1 pkt 2, udziela Zamawiającemu licencje na System lub zapewni udzielenie licencji przez osobę, której przysługują autorskie prawa majątkowe do Systemu. Licencje powinny spełniać co najmniej następujące warunki:
	1. zakres i warunki licencji nie mogą być gorsze od standardowych, oferowanych innym podmiotom przez osobę, której przysługują prawa do Systemu,
	2. powinny obejmować terytorium Rzeczypospolitej Polskiej oraz cały świat.

7. Wykonawca oświadcza, że na podstawie udzielonych licencji Zamawiający otrzyma prawo do korzystania z Systemu, w zakresie umożliwiającym Zamawiającemu korzystanie z niego dla swoich potrzeb, zgodnie z warunkami określonymi przez Producenta, stanowiącymi Załącznik nr 5 do Umowy.

**§6**

**Odpowiedzialność za niewykonanie lub nienależyte wykonanie Umowy**

1. Wykonawca zapłaci Zamawiającemu karę umowną:
2. za odstąpienie Wykonawcy od Umowy z przyczyny niezależnej od Zamawiającego albo w przypadku odstąpienia przez Zamawiającego od Umowy z przyczyny leżącej po stronie Wykonawcy - w wysokości 20% łącznego wynagrodzenia brutto określonego w § 3 ust. 1,
3. w razie opóźnienia w wykonaniu Umowy ponad termin określony w § 2 ust. 2 lub ust. 3 - w wysokości 0,5% wynagrodzenia brutto określonego w § 3 ust. 1 pkt 1, za każdy dzień opóźnienia, chyba że opóźnienie wynika z przyczyn leżących po stronie Zamawiającego,
4. w razie opóźnienia w wykonaniu Umowy ponad termin określony w Formularzu zlecenia - w wysokości 5% wynagrodzenia brutto określonego w formularzu zlecenia, za każdy dzień opóźnienia, chyba, że opóźnienie wynika z przyczyn leżących po stronie Zamawiającego.
5. w przypadku ujawnienia jakiejkolwiek informacji lub innego naruszenia bezpieczeństwa informacji w okresie obowiązywania Umowy lub po wygaśnięciu lub rozwiązaniu Umowy – w wysokości 10 % wynagrodzenia brutto określonego w § 3 ust. 1 za każdy stwierdzony przypadek ujawnienia informacji lub innego naruszenia bezpieczeństwa informacji.
6. w razie opóźnienia w wykonaniu usług gwarancyjnych w zakresie czasów naprawy Systemu opisanych w Załączniku nr 1 - w wysokości:

a) 0,5% wynagrodzenia brutto określonego w § 3 ust. 1 pkt 1, za każdy dzień opóźnienia w usunięciu Awarii Systemu,

b) 0,2% wynagrodzenia brutto określonego w § 3 ust. 1 pkt 1, za każdy dzień opóźnienia w usunięciu Błędu w Systemie,

chyba że opóźnienie wynika z przyczyn leżących po stronie Zamawiającego

1. Zamawiający ma prawo na zasadach ogólnych dochodzić odszkodowania przewyższającego wysokość zastrzeżonej kary umownej.
2. Strony ustalają, iż naliczona przez Zamawiającego kara umowna może być przez niego potrącona z wynagrodzenia należnego Wykonawcy, wskazanego w § 3 ust. 1, na co niniejszym Wykonawca wyraża nieodwołalną zgodę.
3. W przypadku podniesienia przez osoby trzecie przeciwko Zamawiającemu roszczeń związanych z Systemem wykorzystanym do wykonania Przedmiotu Umowy, Wykonawca zobowiązuje się podjąć wszelkie niezbędne czynności prawne i faktyczne w celu zwolnienia Zamawiającego od odpowiedzialności w stosunku do takich osób trzecich. Wykonawca zwróci także Zamawiającemu wszelkie koszty i straty poniesione w wyniku lub w związku z roszczeniami osób trzecich, o których mowa w zdaniu poprzedzającym.

**§7**

**Bezpieczeństwo informacji**

1. Informacją w rozumieniu Umowy są wszystkie dane, materiały lub dokumenty, pisemne, elektroniczne lub ustne, przekazane lub pozyskane przez Wykonawcę w związku z realizacją Umowy oraz wytworzone przez Wykonawcę na potrzeby realizacji Umowy.
2. Informacje stanowią wyłączną własność Ministerstwa Sprawiedliwości.
3. Wykonawca może przetwarzać powierzone mu przez Zamawiającego informacje tylko przez okres obowiązywania Umowy.
4. 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.
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, którymi się posługuje przy realizacji Umowy.
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 lub zniszczeniem.
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 Zamawiającego do odstąpienia od Umowy.
9. Wykonawca może udostępniać informacje jedynie tym swoim pracownikom, 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. Pracownicy Wykonawcy 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 umożliwieniem przystąpienia do prac tym pracownikom.
11. Wykonawca ponosi wszelką odpowiedzialność, tak wobec osób trzecich, jak i wobec Zamawiającego, za szkody powstałe w związku z nienależytą realizacją obowiązków dotyczących 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. Wykonawca może przetwarzać informacje tylko w wersji elektronicznej.
14. 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.
15. Wykonawca zobowiązany jest współpracować z Zamawiającym w odpowiednim zakresie z podmiotami przeprowadzającymi kontrolę.
16. 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.
17. 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:
18. telefonicznie, na numer telefonu ………………………………………………………………………………;
19. na adres email …………………………………………………………………………………………………………..;
20. faksem, na numer ………………………………………………………………………………………………….. .

Powiadomienie dokonane telefonicznie musi zostać potwierdzone poprzez jeden ze sposobów wskazanych w pkt 2 – 3 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:
	1. zapewnić kontrolę nad tym, jakie informacje, kiedy, przez kogo oraz komu są przekazywane, zwłaszcza gdy przekazuje się je za pomocą teletransmisji danych;
	2. zapewnić, aby osoby, o których mowa w pkt 1, zachowywały w tajemnicy informacje oraz sposoby ich zabezpieczeń.
3. Wykonawca nie może powierzyć przetwarzania informacji innym podmiotom bez uprzedniego uzyskania w tym przedmiocie pisemnej zgody Zamawiającego.
4. W przypadku powierzenia przez Wykonawcę informacji, Wykonawca odpowiada za działania i zaniechania tych podmiotów, jak za własne działania lub zaniechania.
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 wykonywanie postanowień umownych przez podwykonawców na takich samych warunkach jak określone w niniejszej Umowie.

**§ 8**

**Gwarancja i rękojmia**

1. Wykonawca udziela Zamawiającemu gwarancji na wdrożony System na okres 12 miesięcy od daty podpisania przez Zamawiającego, bez zastrzeżeń, Protokołu odbioru potwierdzającego należyte wykonanie wdrożenia Systemu.
2. Wykonawca udziela Zamawiającemu gwarancji na wykonane usługi, o których mowa w § 1 ust. 1 pkt 6 na okres 12 miesięcy od daty podpisania Protokołu odbioru tych prac.
3. Wykonawca udziela rękojmi za wady przedmiotu Umowy,
w okresie równym okresowi gwarancji.
4. Uprawnienia gwarancyjne, zgłaszanie awarii przez Zamawiającego, dokonywanie napraw
przez Wykonawcę, określa Załącznik nr 1 do Umowy – Opis przedmiotu zamówienia.

**§ 9**

**Odstąpienie od Umowy**

Zamawiający może odstąpić od umowy, bez konieczności przesyłania dodatkowego wezwania, w przypadku:

* 1. gdy Wykonawca przed wydaniem dokumentów licencyjnych zaprzestał prowadzenia działalności, w przypadku otwarcia likwidacji przez Wykonawcę lub w przypadku wydania sądowego nakazu zajęcia majątku Wykonawcy ;
	2. opóźnienia Wykonawcy w wykonaniu obowiązku wskazanego w § 2 ust. 3 przekraczającego 14 dni.

**§ 10**

**Postanowienia końcowe**

1. Wszelkie zmiany umowy, jej rozwiązanie za zgodą obu stron, odstąpienie od niej lub jej wypowiedzenie wymaga formy pisemnej, pod rygorem nieważności.
2. Prawem właściwym dla Umowy jest prawo polskie.
3. Żadna ze Stron Umowy nie może przenieść praw i obowiązków wynikających z niniejszej Umowy na osobę trzecią bez uprzedniego uzyskania zgody drugiej Strony, wyrażonej w formie pisemnej pod rygorem nieważności.
4. Sądem właściwym do rozstrzygnięcia sporów wynikłych z realizacji postanowień niniejszej Umowy będzie sąd miejscowo właściwy dla siedziby Zamawiającego.
5. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, w tym dwa egzemplarze dla Zamawiającego i jeden dla Wykonawcy.

**Załączniki:**

Załącznik nr 1 - Opis Przedmiotu Umowy.

Załącznik nr 2a - Wzór Protokołu odbioru licencji.

Załącznik nr 2b - Wzór Protokołu odbioru wdrożenia.

Załącznik nr 2c - Wzór Protokołu przeprowadzenia instruktażu stanowiskowego.

Załącznik nr 2d – wzór Formularza zlecenia.

Załącznik 2e – wzór Protokołu odbioru zlecenia.

Załącznik 2f - wzór Protokołu odbioru dokumentacji powykonawczej.

Załącznik nr 3 - Wzór oświadczenia o zachowaniu poufności informacji.

 **ZAMAWIAJĄCY WYKONAWCA**

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

***Załącznik nr 1 do Umowy nr……z dnia….***

**Opis przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa, uruchomienie i wdrożenie systemu klasy SIEM - System do zarządzania informacją i zdarzeniami bezpieczeństwa (SIEM - Security Information and Event Management).

lub

aktualizacji obecnie posiadanego systemu klasy SIEM opisanego w punkcie V opisu przedmiotu zamówienia.

Zamawiający na potrzeby wdrożenia lub aktualizacji posiadanego systemu udostępni infrastrukturę sprzętową na serwerach zwirtualizowanych, wg. specyfikacji uzgodnionych z Wykonawcą. System operacyjny będzie instalowany przez Zamawiającego, natomiast wszystkie czynności związane z wdrożeniem Systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja Systemu przez Wykonawcę odbywać się będzie w siedzibie Zamawiającego. Zamawiający może wyrazić zgodę na wykonanie prac zdalnie w całości lub części.

I. WYMAGANIA FUNKCJONALNE w przypadku zaoferowania innego rozwiązania niż posiadane przez Zamawiającego

1. System musi zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej uwzględniając schematy architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.
2. System musi zawierać bazę wiedzy eksperckiej (KB) uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą.
3. Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.
4. Dostarczone rozwiązanie musi być systemem klasy SOAR (Security Orchestration, Automation And Response) raportowanych przez mechanizmy korelacji zdarzeń. Moduł obsługi incydentów może stanowić integralną część systemu SIEM lub być dostarczony w ramach odrębnego, zintegrowanego z systemem SIEM, rozwiązania.
5. Interfejs systemu elektronicznej dokumentacji musi umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. Wizualizacja musi obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami.
6. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej.
7. System musi prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je usługi i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów (Owners) oraz zespół IT odpowiedzialny za jego obsługę (Custodians).
8. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny (minimum: na podstawie danych pozyskanych z logów oraz poprzez API) lub za pomocą interfejsu graficznego i tabelarycznego.
9. Interfejs interaktywnej mapy sieci musi umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie infrastruktury IT oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT, który został zdefiniowany w elektronicznej dokumentacji.
10. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.
11. System musi pozwalać na dodawanie i przechowywanie załączników powiązanych z obiektami zgromadzonymi w bazie elektronicznej dokumentacji sieci. System powinien akceptować załączniki między innymi w formatach: pdf, MS Word, MS Excel, jpg, png.
12. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja.
13. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.
14. Dla zarejestrowanych zdarzeń/ incydentów system automatycznie wyznaczy ścieżkę ataku i zaprezentuje ją w formie graficznej na schemacie sieci organizacji. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy celem a źródłem zdarzenia lub incydentu.
15. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja.
16. Informacje o procesach muszą uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00).
17. Mechanizmy modułu dokumentacji elektronicznej muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności.
18. System musi pozwalać na zautomatyzowaną ocenę wplywu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku związana z zagrożeniem przełamania zabezpieczeń serwera werbowego organizacji dostępnego z sieci Internet).
19. W ramach obsługi zdarzeń/incydentów/podatności system powinien prezentować informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem oraz ocenę wpływu incydentu na organizację w przypadku materializacji zagrożenia.
20. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla wszystkich systemów IT zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka powinno odbywać się względem zagrożeń natury informatycznej, np.: przełamanie zabezpieczeń, wyciek danych, infekcja złośliwym programem, podsłuch sieciowy.
21. System w razie wykrycia incydentów o wysokim ryzyku materializacji zagrożenia natury technicznej (m.in. przełamanie zabezpieczeń, infekcja złośliwym oprogramowniem) umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.
22. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.
23. System powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie krytycznych usług w organizacji.
24. System ma posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. Interfejs mapy sieci musi pozwalać m.in. na:
	1. wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,
	2. wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia,
	3. wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia,
	4. wyświetlanie lokalizacji zasobów określonego rodzaju,
	5. wyświetlanie najbardziej narażonych zasobów teleinformatycznych,
	6. wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie.
25. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/ incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).
26. Rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE.
27. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń które mają zostać poddane regułom korelacyjnym.
28. System musi umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych.
29. System musi umożliwiać automatyczne dodawanie i usuwanie list referencyjnych na podstawie reguł korelacyjnych umożliwiających zdefiniowanie warunków na podstawie których listy te będą modyfikowane. System musi umożliwiać definiowanie list referencyjnych łączących unikalne wartości w pojedynczym wierszu np: login, adres IP, Aplikacja.
30. System musi być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych system powinien tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla zdarzeń zaobserwowanych w oknie czasowym agregacji.
31. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w scenariuszach obsługi incydentów. Scenariusze obsługi incydentów muszą być uzależnione od ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).
32. System musi umożliwiać wykorzystanie baz reputacyjnych w ramach scenariuszy obsługi incydentów (ang. Playbook).
33. System musi zapewnić graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń, analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą między innymi:
	1. wzbogacanie danych kontekstowych,
	2. gromadzenie artefaktów danych związanych z incydentem,
	3. współpraca z innymi członkami zespołu,
	4. komunikacja w ramach zespołu,
	5. wykonywanie czynności związanych z reakcją na incydent,
	6. raportowanie przebiegu incydentu.
34. System musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów/podatności. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej:  ilość incydentów w czasie w podziale na priorytety, czasy reakcji i obsługi oraz bieżące ilości incydentów obsługiwanych przez poszczególnych użytkowników.
35. System powinien posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook).
36. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
37. System powinien pozwalać na przekazywanie aktywnych linków pomiędzy zintegrowanymi systemami, a otwarcie linku powinno bezpośrednio przekierowywać operatora do konsoli systemu zewnętrznego.
38. System powinien umożliwiać automatyczną zmianę statusu incydentu na podstawie informacji pobranych z innych systemów np.: identyfikacja IOC.
39. System musi umożliwiać zbieranie, przechowywanie i przypisywanie wskaźników kompromitacji (IoC) do incydentów.
40. System powinien udostępniać automatyczny raport z wszystkich podjętych działań w ramach incydentu.
41. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych. Mechanizm musi umożliwiać m.in. parsowanie warunkowe, parsowanie hierarchiczne, wzbogacanie zdarzeń o dodatkowe pola, mapowanie wartości, czy wykorzystanie gotowych parserów przy tworzeniu nowych.
42. Parsowanie warunkowe i hierarchiczne musi być konfigurowalne i obsługiwać następujące metody normalizacji: REGEX, JSON, XML, CEF, LEEF, SYSLOG. Musi umożliwiać wykorzystanie gotowych parserów jako elementów podrzędnych hierarchii oraz wykorzystywanie ich w warunkach.
43. Proces normalizacji musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
44. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
45. System musi zapewnić normalizację (parsowanie) logów protokołami Syslog, TLS Syslog, Netflow, obsługiwać pliki płaskie (ang. flat file), zapytania do bazy danych poprzez sterownik ODBC oraz odbierać wiadomości email.
46. Oferowane rozwiązanie powinno zapewniać możliwość zbierania logów z systemów Microsoft Windows poprzez mechanizm Windows Event Forwarding (WEF) bez konieczności instalowania dedykowanego oprogramowania w tych systemach.
47. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
48. Normalizacja musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól, np. logowanie, wylogowanie, zmiana uprawnień, malware, vulnerability.
49. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
50. System musi posiadać predefiniowany zestaw parserów.
51. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) logów z niestandardowych źródeł danych, w oparciu o składnię wyrażeń regularnych oraz formaty JSON, XML, CIS, LEEF, Syslog. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia.
52. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
53. System musi umożliwiać definiowanie zakresu i czasu uczenia, np.: analiza logowania użytkowników po godzinach pracy, analiza alarmów systemu SIEM. Po wdrożeniu nie będzie wymagane żadne dostrojenie systemu.
54. System musi mieć możliwość wzbogacania kontekstu odbiegającego od normalnego zachowania użytkownika korzystając z danych zewnętrznych, minimum: Threat Intelligence , ActiveDirectory. Przykładowe zastosowanie integracji zakłada wykorzystanie zasobów zewnętrznych, z których dane mogą podnieść skumulowaną ocenę ryzyka dla sesji użytkownika.
55. System musi posiadać funkcję „automatycznej korelacji”, tzn. posiadać zaszyte mechanizmy i reguły korelacji, które po wdrożeniu i „nauce środowiska zamawiającego”, będą przedstawiać właściwe incydenty dla operatorów bez dodatkowej ingerencji w reguły.
56. System musi zapewniać możliwość budowania modeli zachowania użytkowników dla zebranych danych historycznych ze skonfigurowanego (wskazanego) okresu.
57. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych.
58. Dostarczone rozwiązanie musi być objęte 12 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).
59. Rozwiązania SIEM, SOAR, narzędzia elektronicznej dokumentacji (DOC) oraz baza wiedzy (KB) mogą być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań OPZ z poziomu jednej konsoli.
60. Interfejs użytkownika Systemu musi być w języku polskim lub umożliwiać wgranie plików językowych tłumaczących interfejs na język polski. Musi być przejrzysty i konfigurowalny, poprzez pogrupowanie zawartości w bloki tematyczne, co ma umożliwić łatwe i szybkie wyszukiwanie odpowiednich danych.
61. Funkcjonowanie rozwiązania musi być oparta w całości o architekturę „on-premise”, w której przetwarzane dane nie są przesyłane poza infrastrukturę Zamawiającego.
62. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
63. Dopuszczalne jest dostarczenie rozwiązania jako tzw. wirtualnego appliance pod warunkiem ,że obraz appliance jest udostępniany do pobrania przez producenta dostarczonego rozwiązania na jego oficjalnej stronie internetowej w postaci utwardzonego rozwiązania, łącznie z dedykowanym systemem operacyjnym, dla którego Producent regularnie dostarcza aktualizacje, w tym poprawki bezpieczeństwa.
64. System musi zapewniać możliwość współpracy z popularnymi bazami danych, a w tym co najmniej z: MS SQL lub Oracle.
65. System powinien umożliwiać nadawanie uprawnień do obiektów/modułów systemu dla poszczególnych operatorów lub grup operatorów.
66. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
67. System musi dokonywać automatycznej integracji z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach i zasobach zarejestrowanych w domenie AD, minimum to: nazwa użytkownika, login, e-mail, nazwa komputera, przynależność do grup, przełożonego, jednostkę organizacyjną oraz konta uprzywilejowane.
68. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
69. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień do definiowalnych grup odbiorców (co najmniej: powiadamianie email oraz SMS, opcjonalnie czat).
70. System musi być dostępny z poziomu dedykowanego klienta aplikacji lub obsługiwany za pomocą dowolnej przeglądarki internetowej (Chrome, Edge, Firefox), bez konieczności instalowania jakichkolwiek dodatków dla prawidłowego jego działania.
71. System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń.
72. System musi umożliwiać mapowanie zdarzeń korelacyjnych na framework Mitre ATT&CK.
73. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych danych w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.
74. Tworzenie raportów PDF musi posiadać opcje automatycznego harmonogramu, który w zadanym wcześniej momencie pozwoli na wysyłkę utworzonego raportu do zdefiniowanych odbiorców poczty email. Konfiguracja harmonogramu tworzenia raportów PDF i ich wysyłki powinna być dostępna poprzez graficzny interfejs użytkownika.
75. System musi rejestrować i przechowywać pozyskane dane w wersji pierwotnej oraz w wersji znormalizowanej.
76. System musi zapewniać klasyfikację zdarzeń za pomocą notacji punktowej definiującej ich poziom zagrożenia (ryzyko).
77. Interfejs systemu powinien umożliwiać z poziomu jednego okna widoku weryfikację wszystkich działań użytkownika na osi czasu, które spowodowały wzrost ryzyka. Z poziomu tego widoku system umożliwi przejście do opisu konkretnego zdarzenia.
78. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. usługi zagrożone przez incydenty oraz podatności, średni czas obsługi incydentu lub podatności.
79. System pozwoli na prezentację danych w postaci tzw. „Dashboard”, tj. dostosuje zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika.
80. System musi automatycznie wyodrębnić konta użytkowników oraz ich kontekst, minimum przynależność do odpowiednich grup domenowych , konta serwisowe , użytkowników uprzywilejowanych , użytkowników w randze kierowniczej i zarejestrowane stacje robocze celem automatycznej dystrybucji tych danych do odpowiednich narzędzi systemu.
81. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
82. System musi umożliwiać przechowywanie teczek incydentów zawierających dowody, próbki, logi oraz inne powiązane z danym incydentem informacje.
83. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody w teczkach Incydentów.
84. System musi umożliwiać powiązanie każdego zdarzenia/incydentu z odpowiednim priorytetem (definiowanym automatycznie z możliwością manualnej zmiany).
85. System powinien posiadać możliwość rejestracji zgłoszeń i przekształcenia ich w incydenty bezpieczeństwa z możliwością rozdzielenia uprawnień dla obu tych czynności.
86. System powinien mieć logikę automatycznego przypisywania zgłoszeń, minimum na podstawie dostępności operatora, jego obciążenia, oraz cech zasobu którego dotyczy incydent, minimum typ zasobu (np.: serwer lub stacja robocza), krytyczność oraz realizowane z jego udziałem usługi z katalogu usług.
87. System musi umożliwiać grupowanie manualne w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.
88. System powinien grupować automatycznie w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.
89. System powinien umożliwiać obsługę tzw. lawinowych incydentów (incydenty takie same, lecz pochodzące od różnych użytkowników lub systemów) poprzez podłączanie ich do jednego głównego incydentu oraz nadanie odpowiedniego priorytetu tego typu zdarzeniom. Zamkniecie głównego incydentu/zdarzenia powinno umożliwiać zamykanie powiązanych z nim incydentów/zdarzeń w trybie manualnym (operator) lub automatycznym (system). W podglądzie incydentu powinna się pojawić informacja o podpiętych incydentach.
90. System musi pozwalać na określenie automatycznych oraz inicjowanych przez operatora reakcji na incydenty bezpieczeństwa i/lub zdarzenia, polegających na integracji z systemami zewnętrznymi w celu uzyskania dodatkowych informacji, dotyczących incydentu/zdarzenia lub podjęcia akcji zapobiegawczych.
91. System musi umożliwiać wykonywanie działań remediacyjnych na stacjach roboczych/serwerach (pobieranie logów, uruchamianie skryptów, weryfikacja rejestrów, itp.).
92. System musi umożliwiać przypisywanie i przekazywanie incydentów do operatorów lub grup operatorów.
93. System musi pozwalać na zbieranie danych i reputacji z systemów klasy Threat Intelligence minimum to IP, FQDN, URL, Hash.
94. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub/i PowerShell), na skonfigurowanie nowych, nie uwzględnionych przez producentów rozwiązania możliwości integracyjnych z zewnętrznymi systemami.
95. System powinien umożliwiać przeglądanie listy zasobów (urządzeń, systemów, osób, itp.) pod kątem poziomu i ilości incydentów, które są z nimi powiązane.
96. System musi mieć możliwość automatycznego informowania o zmianie statusu incydentu (minimum: wygenerowaniu, przypisaniu, przekroczeniu czasu SLA oraz zamknięciu karty incydentu).
97. System powinien umożliwiać ustawienie parametrów SLA bazując na ustalonym automatycznie priorytecie zdarzania/incydentu/podatności. System musi dokonywać automatycznego pomiaru tych czasów i weryfikacji ich do zdefiniowanych wymagań SLA. Wyniki pomiaru czasu powinny być stale aktualizowane i prezentowane w interfejsie systemu.
98. System powinien umożliwiać dodawanie, modyfikację i usuwanie umów SLA, które zawierają co najmniej następujące parametry: data rozpoczęcia i zakończenia obowiązywania umowy, jednostka organizacyjna (struktura jednostek), której dotyczy umowa, lista usług z katalogu usług, których dotyczy umowa.
99. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej dwóch producentów oraz co najmniej jednym skanerem podatności dostępnym na zasadach open source. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności i importowania jego wyników.
100. Interfejs modułu obsługi incydentów musi prezentować listę podatności zasobów związanych z incydentem.
101. System musi automatycznie ustalać priorytety podatności w odniesieniu do ważności podatnych systemów IT dla organizacji oraz oceny technicznej zagrożenia bazującej na wartości CVSS lub wartości pozyskanej bezpośrednio z silnika skanera.
102. System powinien uwzględniać w ocenie zdarzeń i incydentów, informacje o podatnościach technicznych wykrytych przez narzędzia do zarządzania podatnościami zarówno przez import raportu jak i integrację przez API.
103. System musi zawierać mechanizm definiowania harmonogramów skanowania podatności oraz na ich podstawie automatycznie uruchamiać procesy skanowania i analizowania uzyskanych raportów.
104. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).
105. Rozwiązanie musi posiadać wydajność oraz poziom licencji umożliwiający przetwarzanie zdarzeń na poziomie 2000 EPS.
106. System musi być tak wyskalowany, aby zapewniać możliwość obsługi dla 200 aktualnych źródeł danych znajdujących się w sieci. Przez źródło danych należy rozumieć zasób IT / zasób sieciowy, który zostanie zdefiniowany w systemie oraz będzie objęty jego logiką działania. Przykładowym źródłem danych może być serwer fizyczny, serwer w postaci maszyny wirtualnej, stacja robocza, urządzenie mobilne, switch , router, urządzenia bezpieczeństwa takie jak firewall, IPS, system ochrony anti-malware, strefa sieci obejmująca stacje robocze i inne.
107. Rozwiązanie ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby, które w przyszłości zostaną objęte jego działaniem.

II. WDROŻENIE SYSTEMU

1. Wykonawca w terminie do 20 października 2021 r. będzie odpowiedzialny za dostarczenie, instalację i konfigurację oraz optymalizację środowiska Systemu w infrastrukturze Zamawiającego.
2. Wykonawca przedstawi Zamawiającemu w terminie do 14 dni kalendarzowych po podpisaniu umowy projekt techniczny zawierający w szczególności:
3. Plan i opis architektury logicznej Systemu
4. Opis funkcji Systemu SIEM do zaimplementowania w infrastrukturze Zamawiającego. Szczegółowy opis zakresu integracji Systemu SIEM z innymi systemami eksploatowanymi w infrastrukturze Zamawiającego.
5. Opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Zamawiający, Wykonawca) niezbędnych do dostosowania Systemu do potrzeb Zamawiającego
i konfiguracji środowiska produkcyjnego.
6. Szczegółowy opis koniecznych zmian w konfiguracji urządzeń sieciowych i serwerów Zamawiającego.
7. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:
8. Przedstawienie architektury Systemu
9. Omówienie procedur obsługi administracyjnej Systemu
10. Omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń Systemu
11. Przekazanie informacji na temat konfiguracji i zarządzania Systemem
12. Instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną
13. Zasady realizacji instruktażu stanowiskowego:
14. dla maksimum 6 osób wskazanych przez Zamawiającego
15. łączny wymiar instruktażu stanowiskowego: nie mniejszy niż 3 dni robocze Zamawiającego.
16. instruktaż stanowiskowy będzie prowadzony w siedzibie Zamawiającego lub innym miejscu wskazanym przez Wykonawcę i zaakceptowanym przez Zamawiającego
17. instruktaż stanowiskowy będzie realizowany minimum w oparciu o zakres wykonywanych prac wdrożeniowych Systemu,
18. instruktaż stanowiskowy powinien zostać przeprowadzony w dniach roboczych Zamawiającego, tj. pn – pt, w godzinach 8:15 – 16:15
19. Instruktaż stanowiskowy musi zakończyć się nie później niż do 14 października 2021 roku
20. Osoby prowadzące instruktaż stanowiskowy muszą posiadać wiedzę oraz odpowiednie przygotowanie merytoryczne w zakresie wdrażanego Systemu, a także brać bezpośredni udział we wdrożeniu tego Systemu
21. W ramach realizacji instruktażu stanowiskowego Wykonawca zapewni uczestnikom materiały dydaktyczne w języku polskim (w formie elektronicznej), co najmniej:
22. podręcznik administratora i użytkownika w formie elektronicznej,
23. szczegółowy plan zajęć,
24. opis możliwych do zastosowania rozwiązań: przypadków omawianych w czasie prowadzenia instruktażu oraz najczęściej występujących przypadków przy eksploatacji systemu.

III. DOKUMENTACJA POWYKONAWCZA

1. Wykonawca opracuje i dostarczy Zamawiającemu w terminie do 20 października 2021 r. w formie elektronicznej i papierowej dokument „Dokumentacja powykonawcza".
2. Dokumentacja powykonawcza powinna zawierać następujące elementy:
3. Ogólny opis Systemu SIEM
4. Wykaz całościowy oprogramowania oraz licencji wykorzystywanych w ramach wdrożonego Systemu SIEM
5. Architektura logiczna systemu (graficzna prezentacja systemu i jego połączeń wraz z opisem)
6. Przepływ danych w systemie (koncepcja obiegu informacji w systemie pomiędzy poszczególnymi komponentami, warstwami systemu)
7. Szczegółowa konfiguracja poszczególnych elementów systemu (np. serwery zarządzające, serwery baz danych, systemy operacyjne, serwery aplikacyjne, serwery www - zrzuty ekranów, pliki konfiguracyjne, opisy konfiguracji, opisy uruchomionych usług, opisy poszczególnych funkcji systemu)
8. Polityka aktualizacji systemu i testowania zmian
9. Systemy zależne (np. agenci na innych serwerach, dodatkowe oprogramowanie na innych stacjach roboczych i serwerach współpracujące z systemem, opis integracji z innymi usługami w tym w szczególności z MS Active Directory oraz MS Exchange)
10. Specyfikacja i konfiguracja serwerów wirtualnych
11. Architektura sieciowa systemu (opis połączeń sieciowych pomiędzy poszczególnymi elementami, adresacja IP, umiejscowienie elementów systemu w poszczególnych strefach - DMZ, LAN, Internet)
12. Opis portów komunikacyjnych (opis powinien zawierać informacje o otwartych portach oraz sposób zabezpieczenia zbędnych/nieużywanych portów)
13. Rodzaje kont systemowych i ich uprawnienia (określenie standardowych profili uprawnień, sposobu zarządzania użytkownikami oraz uprawnieniami w systemie)
14. Zarządzanie hasłami (opis sposobu przechowywania haseł w systemie, mechanizmów kryptograficznych wykorzystywanych do ich zabezpieczenia, informacje o przechowywaniu haseł w kodzie programu)
15. Uprawnienia kont serwisowych
16. Role administracyjne
17. Ustawienia polityki haseł
18. Procedury zmiany haseł serwisowych, administracyjnych i użytkownika
19. Procedury weryfikacji uprawnień
20. Konfiguracja reguł firewall
21. Bezpieczeństwo transmisji (opis rozwiązań w zakresie zapewnienia poufności transmisji danych zarówno w sieci LAN/DMZ jak i Internet)
22. Ochrona konfiguracji systemu (ochrona krytycznych plików konfiguracyjnych)
23. Opis rozwiązań w zakresie logowania zdarzeń (wskazanie rodzajów oraz lokalizacji dzienników w systemie, opis logowanych zdarzeń, w przypadku niestandardowych logów opis ich struktury)
24. Ochrona dzienników (opis sposobu zabezpieczenia zapisów w logach przed ich utratą oraz nieuprawnioną zmianą, informacja o czasie przechowywania logów, możliwości przekazania logów do systemów zewnętrznych)
25. Procedura odtwarzania systemu (opisanie procedury backupu i odtworzenia całego systemu i jego poszczególnych elementów, określenie czasu potrzebnego na odtworzenie całego systemu oraz jego poszczególnych elementów, opis procedur przywracania systemu do pełnej funkcjonalności po awarii)
26. Procedura instalacji systemu (opis procedury instalacji systemu „od początku - krok po kroku", opis wszystkich kroków instalacji i konfiguracji systemu w postaci zrzutów ekranu z opisami),
27. Procedury wykonywania krytycznych operacji w systemie (migracja, aktualizacja, itp.)
28. Instrukcje obsługi systemu dla Administratorów.

IV. INNE WARUNKI REALIZACJI ZAMÓWIENIA I GWARANCJA

1. System ma być dostarczony z bezterminową licencją i z wsparciem technicznym obejmującym okres 12 miesięcy od daty podpisania protokołu odbioru wdrożenia Systemu. Wsparcie techniczne obejmuje pomoc przy instalacji systemu oraz przy jego późniejszej eksploatacji. Tj. W ramach wsparcia technicznego Zamawiający ma otrzymać:
	1. bezpłatny dostęp do aktualizacji, poprawek i nowych wersji/kompilacji programu,
	2. wsparcie online 24x7,
	3. wsparcie telefoniczne w godzinach pracy supportu,
	4. dostęp do bazy wiedzy oraz dokumentacji Systemu,
2. Wykonawca udziela gwarancji na wykonane przez Wykonawcę w ramach umowy prace, przez okres 12 miesięcy od dnia podpisania bez zastrzeżeń protokołu odbioru tych prac. W ramach usług gwarancyjnych Wykonawca ma zagwarantować następujące czasy naprawy Systemu licząc od momentu zgłoszenia przez Zamawiającego:
	1. 24 godziny w przypadku Awarii Systemu (jako Awarię Zamawiający definiuje niedostępność systemu lub awarię Systemu, która uniemożliwia jego wykorzystanie)
	2. 72 godzin w przypadku Błędu w Systemie (jako Błąd w systemie Zamawiający definiuje nieprawidłowe działanie systemu lub jego komponentów, które uniemożliwia lub ogranicza prawidłowe działanie Systemu)
3. Problemy z funkcjonowaniem Systemu w ramach gwarancji zgłaszane będą drogą telefoniczną lub mailową lub za pomocą systemu udostępnionego przez Wykonawcę. Wykonawca określi drogę dokonywania zgłoszeń serwisowych oraz przygotuje niezbędne dostępy pozwalające na dokonanie zgłoszenia przez pracowników Zamawiającego. Wykonawca będzie prowadził całą historię złożonych zleceń oraz zapewni Zamawiającemu wgląd do systemu zawierający opis wszystkich zgłoszeń w całym okresie realizacji umowy. Wykonawca zapewni Zamawiającemu możliwość dokonywania zgłoszeń w trybie 24/7. Każde zgłoszenie złożone przez Zamawiającego powinno zawierać:
	1. datę i godzinę zgłoszenia
	2. opis Awarii lub Błędu
	3. sposób naprawy oraz czas realizacji zlecenia.
4. W okresie gwarancji Wykonawca zobowiązany jest do oraz nanoszenia zmian w Dokumentacji powykonawczej związanych z realizacją zadań określonych w pkt. 5. w terminie nie dłuższym niż 10 dni roboczych od dnia dokonania przez Wykonawcę zmian w Systemie. Poprawiona Dokumentacja powinna być dostarczona Zamawiającemu w formie elektronicznej.
5. Wykonawca w ramach asysty zagwarantuje usługi konfiguracji, modernizacji oraz optymalizacji środowiska w liczbie do 320 roboczogodzin. W szczególności:.
	1. Konsultacje w zakresie źródeł danych i procesów związanych z wykrywaniem i reakcją na incydenty
	2. Konsultacje w zakresie wdrożenia systemu zarządzania bezpieczeństwem w oparciu o wdrożony System
	3. Konsultacje w zakresie listy zakresu informacji i danych wymaganych do rozbudowy systemu
	4. Instalacja i konfiguracja dodatkowych kolektorów
	5. Aktualizacje topologii mapy logicznej (wykorzystanie narzędzi: Nmap, WMI, analiza ruchu/logów)
	6. Aktualizacje zasobów informacyjno-usługowych
	7. Uzupełnienie parametrów zasobów informacyjno-usługowych (mechanizmy zabezpieczeń, rodzaje zasobów)
	8. Zmiany w schemacie komunikacji międzystrefowej w ramach kluczowych usług IT (bazy danych, serwery WEB, serwery aplikacyjne, serwery plików, DNS)
	9. Dostrojenie reguł domyślnych oceny ryzyka zaimplementowanych w systemie do organizacji zamawiającego
	10. Dostrojenie reguł zaawansowanych oceny ryzyka zaimplementowanych w systemie do organizacji zamawiającego na podstawie danych przekazanych przez Zamawiającego.
	11. Dostrojenie reguł korelacyjnych zaimplementowanych w systemie do organizacji zamawiającego
	12. Przygotowanie nowych reguł korelacyjnych
	13. Przygotowanie nowych scenariuszy obsługi
	14. Przygotowanie nowych skryptów PowerShell/SSH
6. Zadania realizowane będą każdorazowo na zlecenie Zamawiającego i sumowane na podstawie zrealizowanych godzin (strony wspólnie ustalą każdorazowo ilość godzin koniecznych do zrealizowania zleconego zadania). W ramach zleconego zadania Wykonawca dokona aktualizacji dokumentacji technicznej Systemu, która nie będzie wliczana do ilości godzin poświęconych na zrealizowanie zleconego zadania.

V. AKTUALNIE EKSPLOATOWANE PRZEZ ZAMAWIAJĄCEGO OPROGRAMOWANIE:

Zamawiający aktualnie eksploatuje następujące oprogramowanie:

Secure Visio v2.0

W konfiguracji:

* 1. Maszyna wirtualna pełniąca funkcje kolektora
	2. Maszyna wirtualna pełniąca funkcję konsoli

***Załącznik nr 2a do Umowy nr………… z dnia…..***

Protokół odbioru (wzór)

PROTOKÓŁ ODBIORU LICENCJI

UMOWA NR ……………………………………

Z DNIA ………………………………

Data wykonania : ………………………………………………………….

Data przeprowadzenia odbioru: ………………………………………………………….

Miejsce przeprowadzenia odbioru: ………………………………………………………

Osoby dokonujące odbioru:

Przedstawiciele Zamawiającego: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Przedstawiciele Wykonawcy: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Zgodność wykonania usługi z Umową:

Przekazanie dokumentów licencyjnych:………………………………………………………………..

Wartość brutto oprogramowania/udzielanych licencji: ………………………………….zł (słownie………………………………………………………………………………………………………. zł)

**Upoważniony przedstawiciel Wykonawcy**: **Upoważniony przedstawiciel Zamawiającego:**

 …………………………… ………………………..

***Załącznik nr 2b do Umowy nr z dnia…..***

Protokół odbioru (wzór)

PROTOKÓŁ ODBIORU WDROŻENIA

UMOWA NR ……………………………………

Z DNIA ………………………………

Data wykonania : ………………………………………………………….

Data przeprowadzenia odbioru: ………………………………………………………….

Miejsce przeprowadzenia odbioru: ………………………………………………………

Osoby dokonujące odbioru:

Przedstawiciele Zamawiającego: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Przedstawiciele Wykonawcy: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Zgodność wykonania usługi z Umową:

Wykonanie wdrożenia (instalacji, konfiguracja, integracja oprogramowania: …………………………………………………………………………………………………………………………

**Upoważniony przedstawiciel Wykonawcy: Upoważniony przedstawiciel Zamawiającego**

 …………………………… ………………………..

***Załącznik nr 2c do Umowy nr z dnia…..***

Protokół odbioru (wzór)

PROTOKÓŁ PRZEPROWADZENIA INSTRUKTAŻU STANOWISKOWEGO

UMOWA NR ……………………………………

Z DNIA ………………………………

Data wykonania : ………………………………………………………….

Data przeprowadzenia odbioru: ………………………………………………………….

Miejsce przeprowadzenia odbioru: ………………………………………………………

Osoby dokonujące odbioru:

Przedstawiciele Zamawiającego: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Przedstawiciele Wykonawcy: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Zgodność wykonania usługi z Umową:

Przeprowadzenie instruktażu stanowiskowego dla administratorów zgodnie z §1 ust. 4: ……………………………………………………………………………………………….………………………………

**Upoważniony przedstawiciel Wykonawcy:** **Upoważniony przedstawiciel Zamawiającego:**

 …………………………… ………………………..

***Załącznik nr 2d do Umowy nr z dnia…..***

**ZLECENIE z dnia ……………………………………….**

**dot. umowy nr …………… z dnia …………………………**

|  |
| --- |
| *Wypełnia Zamawiający:* |
| Szczegółowy zakres realizacji zlecenia:  |
| Oczekiwany termin realizacji zlecenia:  |

*………………………..………………………..*

 *(podpis przedstawiciela Zamawiającego)*

|  |
| --- |
| *Wypełnia Wykonawca:* |
| Termin realizacji zamówienia: |
| Pracochłonność - ilość roboczogodzin: |
| Całkowity koszt realizacji zlecenia:  |

*………………………..………………………..*

 *(podpis przedstawiciela Wykonawcy)*

Zamawiający akceptuje wykonanie zlecenia zgodnie z warunkami przedstawionymi przez Wykonawcę / Zamawiający odstępuje od wykonania zlecenia na warunkach przedstawionych przez Wykonawcę\*.

Termin przystąpienia do realizacji zamówienia: ………………………………………….

 *………………………..…………………..……………..*

 *(data i podpis przedstawiciela Zamawiającego)*

*\*niepotrzebne skreślić*

***Załącznik nr 2e do Umowy nr z dnia…..***

Protokół odbioru (wzór)

PROTOKÓŁ ODBIORU REALIZACJI ZLECENIA

UMOWA NR ……………………………………

Z DNIA ………………………………

Data wykonania : ………………………………………………………….

Data przeprowadzenia odbioru: ………………………………………………………….

Miejsce przeprowadzenia odbioru: ………………………………………………………

Osoby dokonujące odbioru:

Przedstawiciele Zamawiającego: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Przedstawiciele Wykonawcy: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Zgodność wykonania usługi wsparcia z zgodnie z §1 ust.6: Umowy:

Ilość zrealizowanych godzin wsparcia dla zleconego zadania *…..(opisać przedmiot/ zakres prac)*…………………………………….………………………………

Ilość pozostałych do wykorzystania godzin wsparcia ……………………………………………..

**Upoważniony przedstawiciel Wykonawcy:** **Upoważniony przedstawiciel Zamawiającego:**

 …………………………… ………………………..

***Załącznik nr 2f do Umowy nr z dnia…..***

Protokół odbioru (wzór)

PROTOKÓŁ ODBIORU DOKUMENTACJI POWYKONAWCZEJ

UMOWA NR ……………………………………

Z DNIA ………………………………

Data wykonania : ………………………………………………………….

Data przeprowadzenia odbioru: ………………………………………………………….

Miejsce przeprowadzenia odbioru: ………………………………………………………

Osoby dokonujące odbioru:

Przedstawiciele Zamawiającego: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Przedstawiciele Wykonawcy: …………………………………………………….

 …………………………………………………….

 …………………………………………………….

Zgodność wykonania usługi z Umową:

Wykonanie dokumentacji powykonawczej: …………………………………………………………………………………………………………………………

**Upoważniony przedstawiciel Wykonawcy: Upoważniony przedstawiciel Zamawiającego**

 …………………………… ………………………..

***Załącznik nr 3 do Umowy nr z dnia…..***

Wzór oświadczenia o zachowaniu poufności

Ja niżej podpisany/a niniejszym oświadczam, że:

1. nie ujawniębezstosownego upoważnienia wydanego przez Ministerstwo Sprawiedliwości, żadnych informacji, w szczególności prawnie chronionych, a także o sposobach zabezpieczenia stosowanych w Ministerstwie Sprawiedliwości, 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 Ministerstwa Sprawiedliwości, innych osób i podmiotów lub naruszenie przepisów prawa, w tym regulacji Ministerstwa Sprawiedliwości, 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:
4. 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),
5. ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412),
6. rozdziału XXXIII ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2017 r., poz. 2204 z późn. zm.).

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

 imię i nazwisko PESEL podpis

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

 miejscowość data

1. Dane osobowe zawarte w oświadczeniu są przetwarzane przez Ministra Sprawiedliwości z siedzibą w Warszawie, Al. Ujazdowskie 11 (00-950), który jest administratorem tych danych osobowych.
2. Dane osobowe zawarte w oświadczeniu są przetwarzane na podstawie art. 6 ust. 1 lit. b  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. Urz. UE L 119 z 04.05. 2016, str. 1).
3. Dane osobowe zawarte w oświadczeniu są przetwarzane w celu wykonania umowy oraz realizacji obowiązków Wykonawcy wynikających z umowy.
4. Dane osobowe zawarte w oświadczeniu nie będą przetwarzane w innym celu niż określony w pkt 3.
5. Dane osobowe zawarte w oświadczeniu nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowych.
6. Dane osobowe zawarte w oświadczeniu będą przechowywane przez okres 50 lat od dnia zakończenia realizacji umowy.
7. Ma Pan/Pani ma prawo żądać od administratora danych osobowych dostępu do danych osobowych zawartych w oświadczeniu, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania, wniesienia sprzeciwu wobec przetwarzania i przenoszenia danych.
8. Odbiorcami danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa.
9. Przysługuje Panu/Pani prawo do wniesienia skargi do Urzędu Ochrony Danych Osobowych z siedzibą przy ul. Stawki 2, 00-193 Warszawa.
10. Dane osobowe zawarte w oświadczeniu nie będą podlegały profilowaniu (zautomatyzowanemu przetwarzaniu)
11. Podanie danych osobowych jest dobrowolne, jednakże odmowa ich podania uniemożliwi realizację przez Pana/Panią obowiązków wynikających z zawartej z Wykonawcą umowy.
12. W sprawach związanych z ochroną danych osobowych należy kontaktować się z Inspektorem Ochrony Danych (iod@ms.gov.pl).