ISTOTNE POSTANOWIENIA UMOWY

§ 1

Przedmiot Umowy

1. W ramach Umowy Wykonawca zobowiązuje się na rzecz Zamawiającego do:
   1) udzielenia lub zapewnienia udzielenia niewyłącznych licencji dla Zamawiającego, na okres 12 miesięcy, 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)
   2) w przypadku zaoferowania innego rozwiązania niż obecnie eksploatowanego przez Zamawiającego
      i. 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;
      ii. udzielenia gwarancji, na oprogramowanie, przez okres 12 miesięcy licząc od daty podpisania przez Zamawiającego bez zastrzeżeń odbioru wdrożonego Systemu , zgodnie z załącznikiem 2b;
      iii. przeprowadzenia instruktażu stanowiskowego dla pracowników Zamawiającego (do 6 administratorów) w zakresie działań administracyjnych dla oprogramowania;
      iv. opracowania i dostarczenia projektu technicznego i dokumentacji powykonawczej.
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 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. Wykonawca zobowiązany jest dokonać wdrożenia lub aktualizacji Systemu, przeprowadzić instruktaż stanowiskowy oraz wykonać dokumentację powykonawczą w terminie do **20 grudnia 2019 r.**, pod warunkiem udostępnienia przez Zamawiającego poprawnie

skonfigurowanej infrastruktury pod wdrożenie lub aktualizacje Systemu.

4. Zamawiający w terminie 2 dni roboczych od otrzymania dokumentacji powykonawczej dokonuje jej akceptacji lub zgłasza do niej uwagi, przesyłając je na adres poczty elektronicznej osób odpowiedzialnymi za realizację Umowy po stronie Wykonawcy.
5. 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. Wykonanie wdrożenia lub aktualizacji, 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, Załącznik nr 2c oraz Załącznik nr 2d** do Umowy.

§ 3

Wynagrodzenie umowne oraz warunki płatności

1. Wynagrodzenie należne Wykonawcy za cały okres realizacji umowy nie przekroczy kwoty **…….. zł brutto** (słownie: …… zł), w tym:
   1) w zakresie przedmiotu umowy określonego w § 1 ust. 1 pkt 1-5 - …….. zł (słownie: ……) brutto,
2. 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.
3. Podstawą do wystawienia faktury, będą łącznie protokoły odbioru stanowiące odpowiednio **Załącznik nr 2a, Załącznik nr 2b, Załączniki nr 2c oraz Załącznik nr 2d** do Umowy, podpisane przez Zamawiającego bez zastrzeżeń.
4. 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.
5. 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 …….
2. Ze strony Wykonawcy osobami odpowiedzialnymi za realizację Umowy oraz upoważnionymi

do kontaktów i do podpisywania protokołów odbioru są :
- ……. tel. ……., e-mail …….
- ……. tel. ……., e-mail …….

3. 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:
    1) 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 % wynagrodzenia brutto określonego w § 3 ust. 1,
    2) 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, za każdy dzień opóźnienia, chyba że opóźnienie wynika z przyczyn leżących po stronie Zamawiającego.
    3) 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.

4) 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, za każdy dzień opóźnienia w usunięciu Awarii Systemu,
   b) 0,2% wynagrodzenia brutto określonego w § 3 ust. 1, za każdy dzień opóźnienia w usunięciu Błędu w Systemie,
5) chyba że opóźnienie wynika z przyczyn leżących po stronie Zamawiającego.

2. Zamawiający ma prawo na zasadach ogólnych dochodzić odszkodowania przewyższającego wysokość zastrzeżonej kary umownej.
3. 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.
4. 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:

1) telefonicznie, na numer telefonu ……;
2) na adres email ……;
3) 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.

18. 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.
19. 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.
20. Wykonawca nie może powierzyć przetwarzania informacji innym podmiotom bez uprzedniego uzyskania w tym przedmiocie pisemnej zgody Zamawiającego.
21. W przypadku powierzenia przez Wykonawcę informacji, Wykonawca odpowiada za działania i zaniechania tych podmiotów, jak za własne działania lub zaniechania.
22. 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.
23. 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 rękojmi za wady przedmiotu Umowy w okresie równym okresowi gwarancji.
3. 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 Protokołu odbioru dokumentacji powykonawczej
Załącznik nr 3 - Wzór oświadczenia o zachowaniu poufności informacji.
Załącznik nr 4 - Wydruk zaświadczenia o wpisie do CEIDG/odpis z KRS.
Załącznik nr 5 - Warunki licencjonowania.

ZAMAWIAJĄCY	**WYKONAWCA**
.....	.....

Załącznik nr 1 do Umowy nr……z dnia….

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest aktualizacja Systemu do najnowszej wersji służącej do skanowania podatności infrastruktury Zamawiającego dla co najmniej 1200 adresów IP oraz roczną licencją dla oferowanego rozwiązania zbudowanego w oparciu o rozwiązania Nexpose RAPID 7 w konfiguracji:

1. Maszyna wirtualna pełniąca funkcję konsoli zarządzającej rozwiązaniem,
2. Maszyna wirtualna pełniąca funkcje silnika skanującego: moduł sieciowy,
3. Maszyna wirtualna pełniąca funkcje silnika skanującego: moduł AppSpider PRO

zgodnego z wymaganiami jak poniżej.

Lub dostawa, uruchomienie i wdrożenie Systemu do skanowania podatności infrastruktury Zamawiającego dla co najmniej 1200 adresów IP oraz roczną licencją dla oferowanego rozwiązania zgodnego z wymaganiami jak poniżej w przypadku zaoferowania rozwiązania innego niż obecnie eksploatowanego przez Zamawiającego. Zamawiający na potrzeby wdrożenia 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 i aktualizacja Systemu przez Wykonawcę odbywać się będzie w siedzibie Zamawiającego. Zamawiający może wyrazić zgodę na wykonanie prac zdalnie w całości lub części.

1. WYMAGANIA w przypadku zaoferowania innego rozwiązania niż posiadane przez Zamawiającego

1.1. Wymagania funkcjonalne

1.1. Architektura

1.1.1. Zarządzanie rozwiązaniem powinno się odbywać przy pomocy przeglądarki

1.1.2. Architektura rozwiązania powinna być w modelu klient (silniki skanujące) / serwer zarządzania (magazyn danych, serwer raportowania)

1.1.3. Skanowanie może być wykonywane z poziomu: serwera (instalacja stand – alone), dowolnego silnika skanującego, chmury (jako opcja)

1.1.4. Rozwiązanie powinno wspierać minimum systemy operacyjne:

- Microsoft Windows 7, 8, 10
- Microsoft Windows Server 2008 (R2), Microsoft Windows Server 2012, Microsoft Windows Server 2012 (R2), Microsoft Windows Server 2016, Microsoft Windows Server 2003
- Red Hat Enterprise Linux 5.x, 6.x, 7.x
- Ubuntu Linux 10.04 LTS, 12.04 LTS
- Oracle Linux
- Centos
- Virtualized Machines on VMware ESXi 5.x, Virtualized Machines on VMware ESXi 6.x VMware vCenter Server 4.x, VMware vCenter Server 5.x, VMware vCenter Server 6.x
- Maszyny wirtualne na Hyber-V 2012/2012R2/2016

1.1.5. Serwer zarządzania powinien dawać możliwość:
- Przechowywania wszystkich danych pochodzących z dowolnego silnika skanującego i testującego
- opierać się na bazie danych PostgreSQL, MSSQL, MYSQL
- Wszystkie dane zebrane przez zewnętrzne silniki skanujące i testujące powinny być przesyłane do centralnej bazy i nie powinny być przechowywane po stronie silników skanujących

1.1.6. Rozwiązanie (zarówno silnik jak i konsola) powinno dawać możliwość wdrożenia, jako:
- Aplikacja
- Maszyna wirtualna
- Rozwiązanie „chmurowe”
- Wszystkie wyżej wymienione sposoby wdrożenia powinny mieć możliwość jednoczesnego uruchomienia w całym środowisku
- Rozwiązanie powinno mieć możliwość pracy w modelu hybrydowym

1.2. Administracja

1.2.1. Przekazywanie danych z silników skanujących i testujących do serwera zarządzania powinno odbywać się bezpiecznym kanałem szyfrowanym SSL

1.2.2. Serwer zarządzania powinien udostępniać możliwość logowania wielu użytkownikom o różnych poziomach dostępu

1.2.3. Różne poziomy dostępu dla użytkowników rozwiązania powinny dawać możliwość definiowania:
- Zmiany zakresu uprawnień do modyfikacji widocznych dla użytkownika hostów
- Poziomów dostępu do raportów
- Możliwości tworzenia raportów
- Obsługi wbudowanego systemu ticketowania

1.2.4. Możliwość wprowadzenia jak największej automatyzacji procesów, powinna obejmować co najmniej:
- Skanowanie i testy o zaplanowanym czasie
- Powiadamianie i alarmowanie administratora o zdefiniowanych zdarzeniach (np. SNMP, Syslog, SMTP)
- Funkcjonalność raportowania powinna mieć możliwość rozszerzenia przy pomocy API producenta rozwiązania
- Tworzenie dynamicznych grup skanowania
- rozwiązanie powinno mieć możliwość wykrywania nowych hostów bez konieczności ich skanowania pod kontem podatności

1.3. Wykrywanie i testowanie podatności

1.3.1. Skanowanie podatności powinno odbywać się na dwa sposoby:
- Skanowanie uwierzytelnione
- Skanowanie bez uwierzytelnienia

1.3.2. Wszystkie testy i skany, które mogą wpłynąć na stabilność działania sprawdzanego hosta, powinny być oznaczone w jasny sposób dla administratora

1.3.3. Skanowanie uwierzytelnione powinno być możliwe, co najmniej przy użyciu:
- Concurrent Versioning System (CVS)
- DB2
- File Transfer Protocol (FTP)
- IBM AS/400
- Lotus Notes/Domino
- Microsoft SQL Server
- Sybase SQL Server

- Microsoft Windows/Samba (SMB/CIFS)
- Microsoft Windows/Samba LM/NTLM Hash (SMB/CIFS)
- MySQL Server
- Oracle
- Post Office Protocol (POP)
- PostgreSQL
- Remote Execution
- Simple Network Management Protocol (SNMP)
- Secure Shell (SSH)
- Secure Shell (SSH) Public Key
- Telnet
- Web Site Form Authentication
- Web Site HTTP Authentication
- Web Site Session Authentication

1.3.4. Rozwiązanie powinno zapewniać wsparcie / obsługę technologii:

- REST
- WSDL
- JSON
- GWT
- JavaScript
- Mobile
- AJAX
- HTML4
- HTML5
- Single Page Applications (SPAs)
- SOAP
- .NET
- Flash Remoting (AMF)
- Silverlight
- Living in the DOM
- Complex Sequences
- CSRF / XSRF Token Tracking

1.3.5. Rozwiązanie powinno wspierać poniżej wymienione mechanizmy autentykacji:

- Simple Form Auth
- SSO
- Macro
- HTTP Auth (Basic, Digest, NTLM)
- Multi-Factor
- CAPTCHA
- Selenium
- Proxy Log
- Session Hijacking
- HMAC
- OAuth
- SSL Client Certificates (Including Smart Cards / CAC Cards)

1.3.6. Rozwiązanie powinno zapewniać kontrole w odniesieniu do wymienionych poniżej kategorii podatności:

- Apache Struts 2 Framework Checks
- Apache Struts Detection

- Arbitrary File Upload
- ASP.NET Misconfiguration
- Autocomplete attribute
- Browser Cache directive (web application performance)
- Browser Cache directive (leaking sensitive information)
- Brute Force (HTTP Auth)
- Brute Force (Form Auth)
- Blind SQL
- Clients Cross-Domain Policy Files
- Information Disclosure in comments
- Cookie attributes
- Cross Origin Resources Sharing (CORS)
- Credentials over an insecure channel
- Cross-Site Request Forgery (CSRF)
- Directory Indexing
- Email Disclosure
- Expression Language Injection
- Forced Browsing
- Sensitive Data Exposure
- Form Session Strength
- FrontPage Checks
- Heartbleed Check
- HTTP Strict Transport Security
- HTTP Authentication over insecure channel
- HTTPS Downgrade
- HTTP Headers
- HTTP Response Splitting
- Information Disclosure in response
- Information Leakage in responses
- Java Grinder
- LDAP Injection
- Local Storage Usage
- Business logic abuse attacks
- Nginx NULL code
- OS Commanding
- Parameter Fuzzing
- Credentials stored in clear text in a cookie.
- Collecting Sensitive Personal Information
- PHP Code Execution
- Privacy Disclosure
- Privilege Escalation
- Profanity
- Reflection
- File Inclusion
- HTTP Verb Tampering
- Predictable Resource Location
- Reverse Clickjacking
- Reverse Proxy
- Information Disclosure in scripts
- Secure and non-secure content mix
- Sensitive data over an insecure channel

- Server Configuration
- Server Side Include (SSI) Injection
- Session Fixation
- Session Strength
- Source Code Disclosure
- SQL Information Leakage
- SQL Injection
- SQL injection Auth Bypass
- SQL Parameter Check
- SSL Strength
- Unvalidated Redirect
- URL rewriting
- ASP.NET ViewState security
- Web Beacon
- Cross-site tracing (XST)
- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection
- XML External Entity Attack
- XPath Injection
- X-Powered-By
- DOM Cross-site scripting (XSS)
- Persistent Cross-site scripting (XSS)
- Reflected Cross-site scripting (XSS)

1.3.7. Rozwiązanie powinno wspierać poniższe opcje konfiguracji skanowania:

- Attack Policy
- Proxy
- Authentication
- Crawler Restrictions
- Attack Restrictions
- HTTP Headers
- Performance
- Reporting
- Web Service
- Recorded Traffic
- Browser Macro
- Selenium Recordings
- Parameters Training
- Custom URLs
- Advanced Options

1.3.8. Rozwiązanie musi umożliwiać tworzenie własnych ataków jak również dawało możliwość przeprowadzania ataku na procesy w obrębie badanych aplikacji.

1.3.9. Rozwiązanie powinno umożliwiać przeprowadzanie tzw. Retestów wobec pojedynczych luk/podatności wykrytych wcześniej w celu sprawdzenia czy zostały one poddane działaniem naprawczym.

1.3.10. Rozwiązanie powinno posiadać funkcjonalność monitorowania , pozwalająca na przeprowadzanie skanów pod kątem przeprowadzonych zmian w zawartości stron internetowych.

1.3.11. Rozwiązanie powinno umożliwiać przetestowanie reguł dla systemów klasy WAF oraz IPS w taki sposób aby zweryfikować, że pożądany ruch sieciowy jest przepuszczony, a nie chciany ruch sieciowy blokowany.

1.3.12. Wykryte podatności powinny być prezentowane w formie pozwalającej na szybkie odniesienie do otwartych baz podatności, takich jak:

- NVD
- Bugtraq
- CERT
- SANS

1.3.13. Używane podczas skanowania podatności testy powinny być zależne od przeprowadzonego wcześniej przez silnik skanowania rozpoznania. Takie rozpoznanie powinno zapewnić inteligentne skanowanie testami podatności dopasowanymi do wykrytego wcześniej systemu operacyjnego oraz aplikacji.

1.3.14. Możliwość śledzenia zmian ryzyka związanego z konkretnym hostem. Powiązanie ryzyka z hostem powinno odbywać się co najmniej na podstawie:

- Adresie IP
- Adresie MAC
- Hostname

1.3.15. Silnik skanujący powinien dostosowywać się do zaistniałej sytuacji i automatycznie wykorzystywać wykryte podatności, na przykład:

- Po wykryciu standardowych danych logowania do rutera, powinny one zostać automatycznie wykorzystane do dalszych testów

1.4. Kontrola aplikacji

1.4.1. Funkcjonalność kontroli aplikacji powinna być standardową częścią rozwiązania

1.4.2. Skanowanie powinno zawierać testy sprawdzające OWASP Top 10

1.4.3. Jeśli aplikacja daje dostęp do systemów back – endowych, rozwiązanie powinno wykorzystać te informacje do dalszego skanowania

1.5. Kontrola baz danych

1.5.1. Funkcjonalność kontroli baz danych powinna być standardową częścią rozwiązania

1.5.2. Wspierane bazy danych, to co najmniej:

- MS SQL/Server versions 6, 7, 2000, 2005, 2008, 2013, 2016
- Oracle 9, 10,11,12
- Sybase Adaptive Server Enterprise (ASE) versions 9, 10 and 11
- DB2
- DB/400
- PostgreSQL versions 6, 7, 8, 9
- MySQL
- MongoDB

1.6. Kontrola polityk bezpieczeństwa (zalecenia konfiguracyjne)

1.6.1. Predefiniowane ustawienia dla skanowania zgodnego z:

- PCI
- HIPPA
- SOX
- SCADA

1.6.2. Skaner konfiguracji powinien być standardową częścią rozwiązania

1.6.3. Powinien zawierać ponad 150 zestawów kontrolnych konfiguracji systemów

1.6.4. Kontrola konfiguracji powinna się odbywać co najmniej wg zaleceń:

- USGCB
- FDCC

- DISA STIG
- CIS

1.7. Raportowanie

1.7.1. Raportowanie musi być niezależne od wykonującego skanowanie/testy silnika (raporty muszą umożliwiać konsolidację wszystkich wyników)

1.7.2. Raporty powinny mieć możliwość generowania przy użyciu:

- Przygotowanych przez producenta wzorców
- Modyfikowanych przez użytkownika standardowych wzorców
- Dodatkowych wzorców raportów pobranych ze stron producenta

1.7.3. Użytkownik powinien mieć możliwość wykonania dowolnego zapytania SQL do bazy danych serwera zarządzania. Wynik takiego zapytania powinien być prezentowany, jako raport w formacie CSV

1.7.4. Raporty powinny mieć możliwość automatycznego generowania wg kalendarza

1.7.5. Raporty powinny mieć możliwość automatycznego doręczania do dedykowanych użytkowników

1.7.6. Raporty powinno dać się generować do następujących formatów (formaty wyjściowe mogą się różnić w zależności od typu raportu):

- PDF
- HTML
- RTF
- XML
- CSV

1.8. Zarządzanie bezpieczeństwem

1.8.1. Ocena ryzyka powinna być możliwa w oparciu o:

- CVSS
- Dedykowany, dynamiczny „Risk Score”

1.8.2. Użytkownika może wpływać na dedykowany „Risk Score” poprzez wprowadzenie rankingu ważności skanowanych hostów

1.8.3. System musi generować dane / raport, pozwalający na przyjęcie strategii podnoszenia bezpieczeństwa firmy. Taki raport powinien zawierać np:

- Sekwencję kroków do podjęcia przez administratorów
- Szacowany czas potrzebny do wykonania operacji
- Instrukcje wykonania operacji
- Ew. linki do pobrania aktualizacji

1.8.4. System musi dawać możliwość dodawania wyjątków z listy podatności

1.9. Integracja

1.9.1. Rozwiązanie powinno się integrować, z zewnętrznymi dostawcami rozwiązań bezpieczeństwa (przy założeniu istnienia udokumentowanych sposobów integracji po stronie tych rozwiązań), a w tym:

- McAfee ESM
- IBM QRadar
- Imperva
- NetIQ
- Micro Focus ArcSight ESM
- Sourcefire
- VMware
- Splunk
- FireMon Risk Analyzer
- McAfee

- Palo Alto
- Rozwiązanie powinno mieć możliwość integracji z wiodącymi systemami klasy WAF, IPS

1.9.2.Rozwiązanie powinno mieć możliwość integracji z VMware, , dająca możliwość:

- Automatyczną aktualizację danych o wirtualnych maszynach
- Skanowanie bezpośrednio przez Hypervisora VMware

1.2. Wdrożenie systemu

1. Wykonawca w terminie do 20 grudnia 2019r będzie odpowiedzialny za dostarczenie, instalację i konfigurację środowiska Systemu w infrastrukturze Zamawiającego.
2. Wykonawca przedstawi Zamawiającemu w terminie do 14 dni kalendarzowych po podpisaniu umowy projekt techniczny zawierający w szczególności:
   1) Plan i opis architektury logicznej Systemu
   2) Opis funkcji Systemu do zaimplementowania w infrastrukturze Zamawiającego. Szczegółowy opis zakresu integracji Systemu z innymi systemami eksploatowanymi w infrastrukturze Zamawiającego.
   3) Opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Zamawiający, Wykonawca) niezbędnych do dostosowania Systemu do potrzeb Zamawiającego i konfiguracji środowiska produkcyjnego.
   4) Szczegółowy opis koniecznych zmian w konfiguracji urządzeń sieciowych i serwerów Zamawiającego.
3. Wykonawca wykona prace implementacyjno-wdrożeniowe obejmujące co najmniej:
   1) wykonanie analizy technicznej i przygotowania projektu technicznego wdrożenia,
   2) Instalacja i konfiguracja rozwiązania,
   3) Konfiguracja i integracja z Active Directory, serwerem DHCP, DNS.
   4) Zdefiniowanie użytkowników systemu,
   5) Przygotowanie min. Trzech skanów podatności i trzech testów aplikacji oraz uruchomienie ich.
   6) Przygotowanie przykładowych raportów,
   7) Implementacja zaprojektowanych polityk, raportów i skanów,
   8) Przeprowadzenie strojenia samego systemu oraz doboru odpowiednich parametrów celem otrzymania najwydajniejszej i najbardziej bezpiecznej konfiguracji systemu,
   9) Przeprowadzanie prac optymalizacji systemu pod kątem minimalizacji liczby fałszywych alertów.

1.3. Dokumentacja powykonawcza

1. Wykonawca opracuje i dostarczy Zamawiającemu w terminie do 20 grudnia 2019 r. w formie elektronicznej i papierowej dokument „Dokumentacja powykonawcza".
2. Dokumentacja powykonawcza powinna zawierać następujące elementy:
   1) Ogólny opis Systemu
   2) Wykaz całościowy oprogramowania oraz licencji wykorzystywanych w ramach wdrożonego Systemu
   3) Architektura logiczna systemu (graficzna prezentacja systemu i jego połączeń wraz z opisem)
   4) Przepływ danych w systemie (koncepcja obiegu informacji w systemie pomiędzy poszczególnymi komponentami, warstwami systemu)

5) 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)
6) Polityka aktualizacji systemu i testowania zmian
7) 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, DHCP, DNS).
8) Specyfikacja i konfiguracja serwerów wirtualnych
9) Architektura sieciowa systemu (opis połączeń sieciowych pomiędzy poszczególnymi elementami, adresacja IP, umiejscowienie elementów systemu w poszczególnych strefach - DMZ, LAN, Internet)
10) Opis portów komunikacyjnych (opis powinien zawierać informacje o otwartych portach oraz sposób zabezpieczenia zbędnych/nieużywanych portów)
11) Rodzaje kont systemowych i ich uprawnienia (określenie standardowych profili uprawnień, sposobu zarządzania użytkownikami oraz uprawnieniami w systemie)
12) Zarządzanie hasłami (opis sposobu przechowywania haseł w systemie, mechanizmów kryptograficznych wykorzystywanych do ich zabezpieczenia, informacje o przechowywaniu haseł w kodzie programu)
13) Uprawnienia kont serwisowych
14) Role administracyjne
15) Ustawienia polityki haseł
16) Procedury zmiany haseł serwisowych, administracyjnych i użytkownika
17) Procedury weryfikacji uprawnień
18) Konfiguracja reguł firewall
19) Bezpieczeństwo transmisji (opis rozwiązań w zakresie zapewnienia poufności transmisji danych zarówno w sieci LAN/DMZ jak i Internet)
20) Ochrona konfiguracji systemu (ochrona krytycznych plików konfiguracyjnych)
21) Opis rozwiązań w zakresie logowania zdarzeń (wskazanie rodzajów oraz lokalizacji dzienników w systemie, opis logowanych zdarzeń, w przypadku niestandardowych logów opis ich struktury)
22) 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)
23) 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)
24) 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),
25) Procedury wykonywania krytycznych operacji w systemie (migracja, aktualizacja, itp.)

26) Instrukcje obsługi systemu dla Administratorów.

1.4. Instruktaż stanowiskowy

Zakres musi obejmować co najmniej poniższe zagadnienia i musi odpowiadać wersji wdrożonego u Zamawiającego Systemu:

1. instalacja i konfiguracja wszystkich modułów oprogramowania,
2. praktyczne wykorzystanie zaimplementowanych funkcjonalności oprogramowania:
    a. tworzenie i zarządzanie zadaniami oraz politykami skanowania,
    b. praktyczne przeprowadzenie różnych rodzajów skanowania, w tym w oparciu o skonfigurowane polityki skanowania,
    c. konfiguracja funkcji badania zgodności, praktyczne przeprowadzenie audytów zgodności,
    d. interpretacja wyników skanowania/audytowania, analiza ryzyka,
    e. konfiguracja funkcji raportowania, generowania raportów,
    f. tworzenie i zarządzanie szablonami raportów,
3. Opis i przedstawienie integracji oprogramowania z usługami Zamawiającego,
4. Zarządzanie wdrożonym oprogramowaniem:
    a. możliwości rozbudowy, przyłączani, odłączanie i konfigurowanie poszczególnych modułów skanujących,
    b. rozwiązywanie problemów powstałych w procesie zarządzania podatnościami,
    c. wykonywanie czynności administracyjnych oraz zadań dotyczących utrzymania wdrożonego oprogramowania.
5. Zasady realizacji instruktażu stanowiskowego:

    a) dla maksimum 6 osób wskazanych przez Zamawiającego
    b) łączny wymiar instruktażu stanowiskowego: nie mniejszy niż 2 dni robocze Zamawiającego.
    c) instruktaż stanowiskowy będzie prowadzony w siedzibie Zamawiającego lub innym miejscu wskazanym przez Wykonawcę i zaakceptowanym przez Zamawiającego
    d) instruktaż stanowiskowy będzie realizowany minimum w oparciu o zakres wykonywanych prac wdrożeniowych Systemu,
    e) instruktaż stanowiskowy powinien zostać przeprowadzony w dniach roboczych Zamawiającego, tj. pn – pt, w godzinach 8:15 – 16:15
    f) Instruktaż stanowiskowy musi zakończyć się nie później niż do 20 grudnia 2018 roku
    g) Osoby prowadzące instruktaż stanowiskowy muszą posiadać wiedzę oraz odpowiednie przygotowanie merytoryczne w zakresie wdrażanego Systemu, a także brać bezpośredni udział we wdrożeniu tego Systemu.
6. W ramach realizacji instruktażu stanowiskowego Wykonawca zapewni uczestnikom materiały dydaktyczne w języku polskim (w formie elektronicznej), co najmniej:
    a) podręcznik administratora i użytkownika w formie elektronicznej,
    a) szczegółowy plan zajęć,
    b) opis możliwych do zastosowania rozwiązań: przypadków omawianych w czasie prowadzenia instruktażu oraz najczęściej występujących przypadków przy eksploatacji systemu.

2. Warunki realizacji zamówienia i gwarancja

1. System ma być dostarczony z 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:
    a. bezpłatny dostęp do aktualizacji, poprawek i nowych wersji/kompilacji programu,
    b. wsparcie online 24x7,
    c. wsparcie telefoniczne w godzinach pracy supportu,
    d. 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:
    a. 24 godziny w przypadku Awarii Systemu (jako Awarię Zamawiający definiuje niedostępność systemu lub awarię Systemu, która uniemożliwia jego wykorzystanie)
    b. 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:
    a. datę i godzinę zgłoszenia
    b. opis Awarii lub Błędu
    c. sposób naprawy oraz czas realizacji zlecenia.

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 nrz 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…..

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 ujawnię bez stosownego 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:
   a) 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),
   b) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412),
   c) 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).