

Projekt umowy na wykonanie skanu bezpieczeństwa aplikacji i systemów IT**UMOWA NR**

zawarta dnia [data] w Koźuchowie pomiędzy Przedsiębiorstwem Usług Komunalnych „USKOM” Sp. z o.o. w Koźuchowie, ul. Elektryczna 9, 67-120 Koźuchów, KRS000096178], NIP 9250003346, REGON970397667, reprezentowanym przez Justynę Antecką-Klimek Prezesa Zarządu zwanym dalej „Zamawiającym”, a [pełna firma, adres, KRS albo CEIDG, NIP, REGON, osoba uprawniona do reprezentacji], zwanym dalej „Wykonawcą”, łącznie zwanymi „Stronami”.

Zamówienie jest realizowane w projekcie „Cyberbezpieczne Wodociągi”, finansowanym ze środków Krajowego Planu Odbudowy i Zwiększania Odporności oraz Unii Europejskiej – NextGenerationEU, inwestycja C3.1.1 „Cyberbezpieczeństwo – CyberPL”.

§ 1 Przedmiot i zakres umowy

1. Wykonawca zobowiązuje się wykonać jednorazową usługę skanowania i analizy podatności bezpieczeństwa systemów, aplikacji oraz infrastruktury IT Zamawiającego, wraz z kontrolowaną weryfikacją wykrytych podatności i sporządzeniem raportu, zgodnie z zapytaniem ofertowym oznaczonym znakiem sprawy wskazanym powyżej, Opisem przedmiotu zamówienia (OPZ), stanowiącym załącznik nr 1 do umowy, oraz ofertą Wykonawcy, stanowiącą załącznik nr 2 do umowy.
2. Badanie obejmuje zasoby IT wskazane przez Zamawiającego, w szczególności serwery, urządzenia sieciowe, systemy operacyjne, usługi sieciowe oraz systemy i aplikacje, w zakresie ilościowym określonym w OPZ i zapytaniu. Wykonawca zidentyfikuje hosty, otwarte porty i usługi oraz ich wersje, jeżeli ich ustalenie jest możliwe przy użyciu standardowych, niedestrukcyjnych metod, znane podatności, nieaktualne oprogramowanie i brakujące aktualizacje bezpieczeństwa, ryzykowne usługi, protokoły i mechanizmy oraz podstawowe błędy i słabości konfiguracji. Przeprowadzi kontrolowaną weryfikację wyników w celu ograniczenia wyników fałszywie dodatnich, oceni ryzyko i wskaże zalecenia. Szczegółowe wymagania określa OPZ.



3. Dokumenty określające zamówienie należy interpretować łącznie, z zachowaniem minimalnych wymagań OPZ i zapytania. W razie rozbieżności pierwszeństwo mają kolejno: umowa, OPZ, zapytanie ofertowe i oferta Wykonawcy. Postanowienia umowy nie mogą być interpretowane jako ograniczenie minimalnych wymagań OPZ lub zapytania. Oferta może przewidywać rozwiązania korzystniejsze dla Zamawiającego, jeżeli nie ograniczają tych wymagań.
4. Wykonawca oświadcza, że posiada wymagane obowiązującymi przepisami uprawnienia, doświadczenie i kwalifikacje do wykonania przedmiotu umowy i czynności z nim związanych, będących przedmiotem umowy, jak również dysponuje niezbędnymi zasobami technicznymi i osobowymi do ich przeprowadzenia.
5. Wykonawca ponosi pełną odpowiedzialność za wszelkie działania i zaniechania, które są zawinione, zarówno własne, swoich pracowników oraz podmiotów, którymi się posługuje lub przy pomocy których wykonuje przedmiotową umowę.

§ 2 Terminy i współdziałanie

1. Wykonawca wykona usługę wraz z przekazaniem kompletnego raportu zgodnego z OPZ do 15 listopada 2026 r.
2. Przed rozpoczęciem badania Wykonawca uzgodni z Zamawiającym zakres, termin i sposób prowadzenia czynności, sposób dostępu do zasobów oraz zasady kontaktu podczas badania. Uzgodnienia obejmą w szczególności czynności mogące powodować zwiększone obciążenie infrastruktury i dopuszczalne okna czasowe ich prowadzenia. Usługa może być realizowana zdalnie lub w siedzibie Zamawiającego, zgodnie z OPZ i uzgodnieniami Stron.
3. Zamawiający przed rozpoczęciem badania przekaze Wykonawcy szczegółową listę zasobów objętych badaniem, w tym adresy IP, nazwy hostów, systemów, urządzeń i usług oraz informacje o konfiguracji niezbędne do realizacji usługi. W razie realizacji zdalnej zapewni uzgodniony sposób dostępu, z zachowaniem obowiązujących u niego zasad bezpieczeństwa. Informacje i dane dostępowe będą przekazywane bezpiecznym kanałem uzgodnionym przez Strony.
4. Wykonawca niezwłocznie poinformuje Zamawiającego o brakach danych lub dostępu, wskazując zakres koniecznego uzupełnienia i przewidywany wpływ na realizację usługi. Zamawiający zapewni współdziałanie niezbędne do wykonania badania. Uzgodnienia organizacyjne i techniczne nie mogą samodzielnie zmieniać zakresu zamówienia, wynagrodzenia ani terminu określonego w ust. 1; ewentualna zmiana umowy podlega § 9 ust. 1.
5. Ilekroć w umowie jest mowa o dniu roboczym, rozumie się przez to dzień od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.



§ 3 Sposób realizacji i bezpieczeństwo badania

1. Wykonawca przeprowadzi badanie z należytą starannością, wykorzystując posiadane doświadczenie i specjalistyczne narzędzia automatyczne, uzupełnione w razie potrzeby manualną weryfikacją wyników. Badanie będzie prowadzone wyłącznie w uzgodnionym zakresie, w sposób bezpieczny i kontrolowany, ograniczający ryzyko wpływu na ciągłość działania, dostępność, wydajność i poprawność funkcjonowania środowiska IT.
2. Zamówienie nie obejmuje pełnego testu penetracyjnego ani działań destrukcyjnych, o ile Zamawiający nie wyrazi na określone czynności odrębnej zgody. Każda taka czynność wymaga uprzedniego określenia jej zakresu i sposobu realizacji oraz zgody Zamawiającego; zgoda nie zastępuje zmiany umowy, jeżeli czynność wymaga takiej zmiany.
3. Bez uprzedniej, wyraźnej zgody Zamawiającego niedopuszczalne są: testy DoS/DDoS i inne działania powodujące celowe przeciążenie systemów lub usług; celowe wyłączanie usług; usuwanie, niszczenie, modyfikowanie lub szyfrowanie danych; trwałe zmiany konfiguracji systemów, urządzeń lub usług; instalowanie dodatkowego oprogramowania, agentów lub komponentów; wykorzystywanie podatności w sposób mogący spowodować zatrzymanie, destabilizację lub utratę dostępności usług oraz inne działania wykraczające poza uzgodniony zakres badania.
4. Jeżeli dalsza weryfikacja podatności mogłaby wiązać się z ryzykiem zakłócenia pracy systemu, Wykonawca przerwie czynności w tym zakresie i poinformuje Zamawiającego. W raporcie wskaże ograniczenia przeprowadzonego badania oraz ustalenia wymagające dalszej weryfikacji.
5. Wykonawca zapewni uprawnienia niezbędne do korzystania z narzędzi wykorzystywanych podczas badania. W zakresie, w jakim raport lub przekazane materiały stanowią utwory, Wykonawca z chwilą ich przekazania udziela Zamawiającemu, w ramach wynagrodzenia określonego w § 5 ust. 1, niewyłącznej licencji na czas nieoznaczony, bez ograniczeń terytorialnych. Licencja obejmuje utrwalanie i zwielokrotnianie całości lub części materiałów techniką drukarską i cyfrową, zapisywanie w pamięci komputerów oraz przechowywanie w systemach informatycznych Zamawiającego. Zamawiający może udostępniać materiały podmiotom działającym na jego rzecz przy usuwaniu lub ograniczaniu podatności, audytorom oraz instytucjom uprawnionym do rozliczenia i kontroli projektu, a także upoważniać je do korzystania z materiałów w zakresie niezbędnym do tych czynności, z zachowaniem poufności. Wykonawca zapewnia posiadanie praw niezbędnych do udzielenia powyższych uprawnień.

§ 4 Raportowanie i odbiór

1. Wykonawca prześle raport w formie elektronicznej, np. w formacie PDF. Raport musi zostać sporządzony w języku polskim. Raport będzie zawierał co najmniej: zakres badania, zastosowaną metodykę i narzędzia, wykaz przebadanych zasobów, opis podatności, słabości i nieprawidłowości, poziom ryzyka każdego ustalenia, odniesienia do CVE i CVSS, jeżeli mają zastosowanie, dowody umożliwiające weryfikację ustaleń, zalecenia oraz podsumowanie zagrożeń wymagających priorytetowych działań. Podatności i słabości zostaną sklasyfikowane co najmniej na poziomach: krytyczny, wysoki, średni, niski i informacyjny, z uwzględnieniem wpływu na poufność, integralność i dostępność systemów i danych. Jeżeli dostępna jest ocena CVSS, Wykonawca wskaże wartość punktową oraz, w miarę możliwości, wektor CVSS; pozostałe ustalenia sklasyfikuje na podstawie oceny eksperckiej, z krótkim uzasadnieniem. W raporcie wskaże również przypadki, w których ustalenie wersji oprogramowania lub usług nie było możliwe.
2. Podstawą odbioru będzie przekazanie kompletnego raportu zgodnego z OPZ. Zamawiający sprawdzi jego kompletność, zgodność z zakresem zamówienia oraz czytelność ustaleń i zaleceń. Odbiór nastąpi po zaakceptowaniu raportu przez Zamawiającego i zostanie potwierdzony protokołem odbioru podpisanym przez upoważnionych przedstawicieli Stron; dopuszcza się podpis elektroniczny.
3. Zamawiający prześle akceptację raportu albo uwagi wymagające wyjaśnienia lub uzupełnienia w ciągu 3 dni roboczych od otrzymania raportu zgłoszonego do odbioru. Brak odpowiedzi nie oznacza automatycznej akceptacji. Wykonawca wyjaśni lub uzupełni stwierdzone braki, nieścisłości lub konieczność doprecyzowania wyników bez dodatkowego wynagrodzenia, w terminie nie dłuższym niż 3 dni robocze od przekazania uwag, chyba że Zamawiający wyrazi zgodę na inny termin. Po uzupełnieniu raportu Wykonawca ponownie zgłosi usługę do odbioru.
4. Na żądanie Zamawiającego Wykonawca udzieli wyjaśnień dotyczących raportu oraz omówi zidentyfikowane podatności, poziomy ryzyka i zalecenia dotyczące ich usunięcia lub ograniczenia, bez dodatkowego wynagrodzenia.
5. Za datę wykonania usługi na potrzeby oceny zachowania terminu określonego w § 2 ust. 1 uznaje się datę przekazania Zamawiającemu kompletnego raportu zgodnego z OPZ, którego zgodność została potwierdzona w toku odbioru. Późniejsza data akceptacji raportu lub podpisania protokołu odbioru nie zmienia tej daty. Jeżeli osiągnięcie zgodności raportu z OPZ wymagało jego uzupełnienia lub poprawienia, za datę wykonania usługi uznaje się datę przekazania raportu uwzględniającego te uzupełnienia lub poprawki.



§ 5 Wynagrodzenie i zapłata

1. Za prawidłowe wykonanie całego przedmiotu umowy Zamawiający zapłaci Wykonawcy wynagrodzenie ryczałtowe zgodne z ofertą, w łącznej wysokości [kwota] zł (słownie: [uzupełnić]), stanowiącej całkowitą kwotę do zapłaty, z uwzględnieniem VAT, jeżeli ma zastosowanie. W przypadku opodatkowania VAT: wartość netto wynosi [kwota] zł, stawka VAT [stawka]%, kwota VAT [kwota] zł, a wartość brutto [kwota] zł. W przypadku zwolnienia z VAT należy wskazać „zw.” i podstawę zwolnienia: [uzupełnić]. Jeżeli VAT nie ma zastosowania, należy wskazać „nie dotyczy”; wówczas wynagrodzenie nie jest powiększane o VAT.
2. Wynagrodzenie obejmuje wszystkie koszty realizacji umowy i OPZ, w tym uzgodnienia organizacyjne i techniczne, skanowanie, analizę i kontrolowaną weryfikację podatności, wykorzystanie narzędzi, sporządzenie i bezpieczne przekazanie raportu, wymagane wyjaśnienia, omówienie wyników oraz uzupełnienie raportu. Wykonawca nie pobierze odrębnych opłat za te elementy.
3. Warunkami zapłaty wynagrodzenia są podpisanie protokołu odbioru bez zastrzeżeń oraz doręczenie Zamawiającemu prawidłowo wystawionego lub sporządzonego dokumentu rozliczeniowego właściwego dla statusu Wykonawcy. Zapłata nastąpi przelewem w terminie 14 dni od dnia spełnienia ostatniego z tych warunków. Dokument rozliczeniowy wystawia się zgodnie z obowiązującymi przepisami. Zamawiający przed jego wystawieniem przekaze Wykonawcy dane niezbędne do prawidłowego rozliczenia.
4. Strony stosują obowiązujące przepisy dotyczące fakturowania oraz mechanizmu podzielonej płatności, jeżeli znajdują zastosowanie. Za dzień zapłaty uważa się dzień obciążenia rachunku Zamawiającego.

§ 6 Dane osobowe, poufność i dokumentacja projektu

1. Wykonawca zachowa w poufności wszelkie informacje uzyskane w związku z realizacją umowy, w szczególności dotyczące architektury środowiska IT, adresacji, konfiguracji, wykrytych podatności i danych uwierzytelniających. Wykorzysta je wyłącznie w celu wykonania umowy, zapewni dostęp jedynie osobom upoważnionym i zastosuje odpowiednie środki organizacyjne oraz techniczne chroniące je przed nieuprawnionym dostępem, utratą, ujawnieniem lub modyfikacją. Informacje nie będą udostępniane osobom trzecim bez uprzedniej zgody Zamawiającego, z wyjątkiem ujawnienia wymaganego przez prawo. Obowiązek poufności trwa także po zakończeniu umowy i nie obejmuje informacji, które stały się publicznie dostępne w sposób zgodny z prawem, bez naruszenia obowiązków Wykonawcy.



2. Jeżeli Wykonawca będzie przetwarzać dane osobowe w imieniu Zamawiającego, Strony przed rozpoczęciem takiego przetwarzania zawrą odrębną umowę powierzenia zgodną z art. 28 RODO. Umowa powierzenia określi w szczególności instrukcje, środki bezpieczeństwa, dalsze powierzenie, incydenty, retencję oraz zwrot albo usunięcie danych. Samo podpisanie niniejszej umowy nie zastępuje powierzenia. Przed rozpoczęciem przetwarzania Wykonawca przekaze informacje o miejscu przetwarzania danych oraz podmiotach, z których usług korzysta w tym zakresie. Przekazanie danych poza Europejski Obszar Gospodarczy może następować wyłącznie zgodnie z wymaganiami RODO.
3. Wykonawca udostępni Zamawiającemu dokumenty i wyjaśnienia niezbędne do wykazania wykonania usługi, rozliczenia projektu oraz uprawnionych kontroli dotyczących tej usługi, z zachowaniem zasad poufności, przepisów prawa i umowy powierzenia, jeżeli została zawarta.
4. Raport, wyniki skanowania, dane dostępne oraz pozostałe materiały zawierające informacje o podatnościach lub konfiguracji środowiska będą przechowywane i przekazywane w sposób zabezpieczony przed dostępem osób nieuprawnionych. Jeżeli materiały zostaną zabezpieczone hasłem lub innym sekretem, dane umożliwiające ich odszyfrowanie zostaną przekazane Zamawiającemu odrębnym kanałem komunikacji.
5. Po zakończeniu realizacji usługi i przekazaniu wymaganej dokumentacji Wykonawca w terminie 14 dni od odbioru raportu usunie dane i materiały oraz złoży pisemne oświadczenie o ich usunięciu kopie danych i materiałów pozyskanych podczas badania, chyba że dalsze przechowywanie wynika z obowiązujących przepisów prawa lub zostanie odrębnie uzgodnione z Zamawiającym. W odniesieniu do danych osobowych zastosowanie mają również postanowienia umowy powierzenia, jeżeli została zawarta.

§ 7 Osoby do kontaktu

1. Ze strony Zamawiającego: Piotr Malczyk, 509-598-643 p.malczyk@uskom.eu, ze strony Wykonawcy: [imię i nazwisko, telefon, adres e-mail]. Osoby te koordynują realizację i podpisują protokoły, jeśli otrzymały odpowiednie upoważnienie.
2. Zmiana danych kontaktowych wymaga zawiadomienia drugiej Strony i nie stanowi zmiany umowy. Oświadczenia o odstąpieniu lub zmianie umowy składają osoby uprawnione do reprezentacji.

§ 8 Kary umowne i zakończenie umowy

1. Za zwłokę Wykonawcy w wykonaniu usługi wraz z przekazaniem kompletnego raportu w terminie określonym w § 2 ust. 1 Zamawiający może naliczyć karę umowną w wysokości 0,2% łącznego wynagrodzenia ryczałtowego określonego w § 5 ust. 1 za każdy dzień zwłoki.



2. Za zwłokę w wyjaśnieniu lub uzupełnieniu raportu po terminie określonym zgodnie z § 4 ust. 3 Zamawiający może naliczyć karę umowną w wysokości 0,2% łącznego wynagrodzenia ryczałtowego określonego w § 5 ust. 1 za każdy dzień zwłoki. Za odstąpienie od umowy z przyczyn leżących po stronie Wykonawcy kara wynosi 10% tego wynagrodzenia. Łączna wysokość kar umownych nie przekroczy 20% łącznego wynagrodzenia ryczałtowego określonego w § 5 ust. 1.
3. Jeżeli zwłoka w wykonaniu usługi wraz z przekazaniem kompletnego raportu przekroczy 7 dni roboczych, Zamawiający może wyznaczyć dodatkowy odpowiedni termin, nie krótszy niż 3 dni robocze, z zagrożeniem odstąpienia od umowy po jego bezskutecznym upływie. Po bezskutecznym upływie tego terminu Zamawiający może odstąpić od umowy. Taką samą procedurę stosuje się do istotnej wady usługi lub raportu uniemożliwiającej odbiór. Oświadczenie o odstąpieniu wymaga formy pisemnej albo elektronicznej z kwalifikowanym podpisem.
4. Strony zachowują prawo dochodzenia odszkodowania przenoszącego kary do wysokości rzeczywiście poniesionej szkody na zasadach ogólnych. Naliczanie kar nie wyłącza obowiązku wykonania świadczenia, chyba że umowa zostanie zakończona.
5. Zamawiający ma prawo do potrącenia należnych mu kar umownych z wynagrodzenia przysługującego Wykonawcy, na co Wykonawca wyraża zgodę.

§ 8a Odpowiedzialność Wykonawcy

1. Wykonawca odpowiada za szkody wyrządzone Zamawiającemu w związku z wykonywaniem umowy, w tym przez osoby, którymi się posługuje.
2. Wykonawca zobowiązuje się posiadać przez cały okres realizacji umowy ubezpieczenie odpowiedzialności cywilnej z tytułu prowadzonej działalności na kwotę nie niższą niż 500 000,00zł i okazać polisę na żądanie Zamawiającego.
3. Wykonawca nie może powierzyć wykonania usługi lub jej części podwykonawcy bez uprzedniej pisemnej zgody Zamawiającego.
4. Wykonawca nie może zbywać na rzecz osób trzecich wierzytelności wynikających z niniejszej umowy, w tym do wynagrodzenia, bez uprzedniej pisemnej zgody Zamawiającego, wyrażonej w formie pisemnej pod rygorem nieważności.

§ 9 Postanowienia końcowe

1. Zmiana umowy wymaga formy pisemnej albo elektronicznej z kwalifikowanymi podpisami pod rygorem nieważności, z wyjątkiem zmiany danych kontaktowych. Zmiana nie może ograniczać wymagań OPZ ani prowadzić do nieuprawnionej zmiany zakresu lub ceny w projekcie.
2. W sprawach nieuregulowanych przedmiotową umową stosuje się odpowiednio Kodeks cywilny i inne przepisy prawa powszechnie obowiązującego.



3. Umowę sporządzono w języku polskim i podlega prawu polskiemu.
4. Strony zobowiązują się do podjęcia próby polubownego rozwiązania wszelkich sporów wynikających z niniejszej umowy przed wystąpieniem do sądu.
5. W przypadku powstania sporu, Strona, która go zgłasza, jest zobowiązana do pisemnego poinformowania drugiej Strony o przedmiocie sporu oraz zaproponowania terminu spotkania w siedzibie Zamawiającego w celu jego wyjaśnienia i podjęcia rozmów.
6. Strony ustalają, że spotkanie w celu polubownego rozwiązania sporu powinno odbyć się w terminie nie dłuższym niż 10 dni roboczych od dnia doręczenia wezwania.
7. Strony zobowiązują się do poddania sporu w sprawach, w których zawarcie ugody jest dopuszczalne, mediacjom lub innemu polubownemu rozwiązaniu sporu przed Sądem Polubownym przy Prokuraturii Generalnej Rzeczypospolitej Polskiej, wybranym mediatorem albo osobą prowadzącą inne polubowne rozwiązywanie sporów.
8. W przypadku braku ugody lub polubownego rozstrzygnięcia sporu, spory rozstrzyga sąd powszechny właściwy dla siedziby Zamawiającego.
9. W przypadku, gdy którekolwiek postanowienie przedmiotowej umowy zostanie uznane za nieważne, bezskuteczne lub niemożliwe do wyegzekwowania, w całości lub części, nie wpłynie to na ważność, skuteczność lub możliwość wyegzekwowania pozostałych postanowień przedmiotowej umowy.
10. Strony zgadzają się zastąpić takie postanowienie innym postanowieniem wynegocjowanym w dobrej wierze, które, na ile jest to możliwe, osiąga pierwotny cel ekonomiczny Stron.
11. Strony oświadczają, że w razie stwierdzenia ewentualnej nieważności poszczególnych postanowień przedmiotowej umowy zostałaaby ona zawarta bez tych postanowień.
12. Nagłówki poszczególnych paragrafów mają charakter jedynie pomocniczy i nie wpływają na wykładnię poszczególnych postanowień przedmiotowej umowy.
13. Załączniki do przedmiotowej umowy stanowią jej integralną część. Wykonawca zobowiązany jest uwzględnić i przestrzegać dokumenty stanowiących załączniki do umowy.
14. Integralną częścią umowy są: załącznik nr 1 – OPZ „Skan bezpieczeństwa aplikacji i systemów IT”, załącznik nr 2 – oferta Wykonawcy oraz zapytanie ofertowe oznaczone znakiem sprawy wskazanym powyżej. Numeracja załączników do umowy jest odrębna od numeracji załączników do zapytania ofertowego. Odrębna umowa powierzenia zostanie zawarta, jeżeli będzie wymagana. Umowę sporządzono w dwóch egzemplarzach albo podpisano elektronicznie.
15. Umowę odczytano, zgodnie przyjęto i podpisano.

ZAMAWIAJĄCY

WYKONAWCA

Rodca Prawny
Mateusz Wartalski
ZG-35

14.10.2026