ZAMAWIAJĄCY:

Spółka Komunalna Dorzecze Białej Sp. z o.o.
ul. Jana III Sobieskiego 69 C, 33-170 Tuchów
NIP 993-040-66-00

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Na potrzeby postępowania zakupowego pn.: „Dostawa oprogramowania klasy GRC oraz zapewnienie dostępu do platformy szkoleniowej z zakresu cyberbezpieczeństwa" w ramach projektu „Cyberbezpieczne Wodociągi" Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo: „Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi". Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności.

Spis treści

Wymagania ogólne 2
1. System klasy GRC do zarządzania ryzykiem i SZBI – 1 licencja 3
2. Platforma szkoleniowa z zakresu cyberbezpieczeństwa – 31 użytkowników, 12 miesięcy 6

Wymagania ogólne

W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę/Producenta, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne".

Za rozwiązanie równoważne Zamawiający uzna produkt lub usługę, które spełniają wszystkie parametry techniczne, funkcjonalne i użytkowe wskazane w SOPZ jako minimalne, zapewniają pełną kompatybilność z posiadaną przez Zamawiającego infrastrukturą sprzętowo-programową, nie powodują obniżenia poziomu bezpieczeństwa, wydajności, niezawodności ani funkcjonalności w stosunku do rozwiązania opisanego w SOPZ oraz posiadają certyfikaty i deklaracje zgodności równoważne wymaganym w SOPZ.

Wykonawca, który powołuje się na rozwiązania równoważne, jest obowiązany wykazać w treści oferty, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego. W tym celu Wykonawca zobowiązany jest złożyć wraz z ofertą przedmiotowe środki dowodowe, o których mowa w SWZ, tj. karty techniczne lub alternatywny opis funkcji oferowanych systemów, potwierdzające spełnienie wymagań, o których mowa powyżej.

Okresy licencji, subskrypcji i wsparcia wskazane w opisie poszczególnych pozycji stanowią okresy minimalne. O ile inaczej nie zaznaczono, wszelkie zapisy SOPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.

Przedmiot zamówienia obejmuje dostawę oprogramowania klasy GRC wraz z licencją oraz zapewnienie Zamawiającemu dostępu do platformy szkoleniowej z zakresu cyberbezpieczeństwa, wraz z usługami wsparcia i pomocy technicznej określonymi w opisie poszczególnych pozycji. Siedziba Zamawiającego: ul. Jana III Sobieskiego 69 C, 33-170 Tuchów.

1. System klasy GRC do zarządzania ryzykiem i SZBI – 1 licencja

Parametr / funkcja	Wymaganie minimalne
Postanowienia ogólne	
Przeznaczenie	Oprogramowanie wspomagające zarządzanie w zakresie bezpieczeństwa informacji.
Wersja i język	Oprogramowanie dostarczone w najnowszej wersji, w języku polskim.
Dokumentacja	Oprogramowanie posiada dokumentację użytkownika opisującą funkcjonalność każdego z modułów oprogramowania oraz dokumentację administratora opisującą sposób administrowania programem, w tym jego instalowania, konfiguracji, sposobu tworzenia kopii zapasowych oraz odtwarzania w przypadku awarii.
Wymagania ogólne i środowisko pracy	
Kompletność dostawy	Koszt zakupu oprogramowania uwzględnia koszt wszystkich składników oprogramowania (poza systemem operacyjnym zainstalowanym na serwerze Zamawiającego), które są niezbędne do jego pracy zgodnie z niniejszą specyfikacją.
Zakres dostawy	W ramach zamówienia Zamawiający otrzyma wersję instalacyjną oprogramowania oraz licencję uprawniającą do korzystania z przedmiotowego oprogramowania.
Architektura aplikacji	Program pracuje jako aplikacja intranetowa, uruchamiana i prawidłowo pracująca w aktualnych wersjach przeglądarek internetowych (MS Edge, Google Chrome, Firefox).
Centralne przechowywanie danych	Wszystkie dane gromadzone w oprogramowaniu zapisywane są wyłącznie centralnie, na komputerze pełniącym rolę serwera pracującego w trybie ciągłym przez 24 godziny na dobę.
Serwer	Serwer dostarcza Zamawiający; serwer znajduje się w jego siedzibie.
Praca w środowisku Linux	Aplikacja ma możliwość uruchomienia na serwerze pracującym pod systemem Linux (konfiguracja instalacji niestandardowych powinna być określona w dokumentacji programu).
Funkcjonalność oprogramowania (oprogramowanie musi:)	
Rejestr procesów	Posiadać rejestr zidentyfikowanych procesów, w tym procesów z zakresu ochrony danych.
Rejestr komórek organizacyjnych	Posiadać rejestr komórek organizacyjnych, który będzie oparty na regulaminie organizacyjnym.
Opis komórki organizacyjnej	Posiadać możliwość opisu komórki organizacyjnej poprzez określenie jej podrzędności w strukturze organizacyjnej, przypisania do niej stanowisk pracy oraz zakresu zadań, jaki realizuje.
Rejestr pracowników	Posiadać rejestr wszystkich pracowników, praktykantów i stażystów oraz osób świadczących pracę na umowach cywilnoprawnych.
Rejestr aktywów informacyjnych	Umożliwiać prowadzenie rejestru zidentyfikowanych aktywów informacyjnych oraz zasobów wspomagających.
Opisywanie aktywów	Wspomagać opisywanie aktywów, m.in. poprzez wskazanie procesów przetwarzających informacje oraz istotności informacji dla realizacji danego procesu, wskazanie zasobów wykorzystywanych przy przetwarzaniu informacji oraz określenie poziomu istotności zasobu dla informacji.
Klasyfikacja aktywów	Umożliwiać ustalenie wymaganego poziomu podstawowych oraz dodatkowych atrybutów informacji i adekwatnie do tego ustalać klasyfikację aktywów.
Rejestr czynności przetwarzania	Umożliwiać prowadzenie, zgodnie z przepisami prawa, rejestru czynności przetwarzania i kategorii czynności przetwarzania danych osobowych w Jednostce Zamawiającego.
Klauzule informacyjne	Posiadać możliwość rejestrowania klauzul informacyjnych.
Umowy powierzenia	Posiadać możliwość ewidencji zawartych umów powierzenia przetwarzania danych osobowych.
Upoważnienia do przetwarzania	Wspomagać wystawianie upoważnień do przetwarzania danych osobowych oraz prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych.

Parametr / funkcja	Wymaganie minimalne
Uprawnienia do systemów informatycznych	Wspomagać wystawianie uprawnień do systemów informatycznych.
Zestawienie uprawnień	Generować zestawienie uprawnień do systemów informatycznych z kryterium użytkownik lub program.
Rejestr ryzyk	Posiadać rejestr zidentyfikowanych ryzyk w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych.
Zarządzanie ryzykiem	Posiadać możliwość identyfikacji i ewidencji czynników ryzyka, podatności na zagrożenia lub szanse, opisania skutków ryzyka, estymacji i oceny ryzyka, ustalenia reakcji na ryzyko oraz monitorowania i raportowania ryzyka.
Cykliczna ocena ryzyka	Posiadać możliwość przeprowadzania cyklicznej oceny ryzyka.
Prezentacja ryzyka	Prezentować ryzyka w formie graficznych zestawień, m.in. mapy ryzyka.
Rejestr aplikacji	Posiadać rejestr wszystkich użytkowanych aplikacji.
Elektroniczne wnioskowanie o uprawnienia	Posiadać możliwość elektronicznego wnioskowania o nadanie właściwych uprawnień dla pracowników zgodnie z ich zakresem obowiązków do obsługi programów komputerowych.
Rejestr incydentów i słabości	Posiadać rejestr zaistniałych incydentów oraz słabości systemu.
Obsługa incydentów	Wspomagać obsługę incydentów bezpieczeństwa informacji, w tym określenie operatora incydentu, oraz ewidencjonować podejmowane działania.
Zestawienia incydentów	Posiadać stosowne zestawienia dotyczące zidentyfikowanych incydentów i słabości systemów.
Rejestr certyfikatów bezpieczeństwa	Posiadać rejestr certyfikatów bezpieczeństwa.
Wnioskowanie o certyfikat	Posiadać możliwość wnioskowania o nadanie certyfikatu bezpieczeństwa.
Ewidencja certyfikatów	Umożliwiać ewidencjonowanie certyfikatów bezpieczeństwa.
Rejestr audytów wewnętrznych	Posiadać rejestr przeprowadzonych audytów wewnętrznych, w tym audytów w zakresie bezpieczeństwa informacji i ochrony danych osobowych.
Rejestr niezgodności	Posiadać rejestr wszystkich zidentyfikowanych nieprawidłowości (niezgodności) w zakresie bezpieczeństwa informacji i ochrony danych osobowych.
Działania korygujące	Możliwość określenia działań korygujących i korekcyjnych względem zidentyfikowanej nieprawidłowości oraz zgłaszania wykonania działań korygujących.
Rejestr przeglądów zarządzania	Posiadać rejestr przeprowadzanych w Jednostce Zamawiającego cyklicznych przeglądów zarządzania w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych.
Automatyczne raportowanie	Możliwość automatycznego przygotowania raportu do analizy z zakresu m.in. bezpieczeństwa informacji i ochrony danych osobowych.
Powiązanie modułów	
Kompatybilność modułów	Wszystkie moduły programu muszą być ze sobą kompatybilne i wzajemnie powiązane (moduły korzystają z danych wprowadzanych w innych modułach bez konieczności ponownego ewidencjonowania tych samych danych).
Licencja	
Zakres licencji	Licencja dostarczona powinna być w modelu wieczystym (bezterminowym) - Licencja zezwala na jednoczesną pracę w programie wszystkich pracowników Jednostki Zamawiającego.
Brak limitu końcówek	Licencja nie może ograniczać liczby końcówek jednocześnie korzystających z oprogramowania.
Kopie testowe/szkoleniowe	Licencja musi dopuszczać tworzenie przez Zamawiającego dowolnej ilości kopii oprogramowania dla celów testowych lub szkoleniowych.
Wsparcie	Oprogramowanie powinno mieć bazowe (natywne) wsparcie, w ramach którego Zamawiający zostanie uprawniony do nieodpłatnego pobierania poprawek i aktualizacji oraz do bieżącej pomocy (nadzoru) w obsłudze programu.

Parametr / funkcja	Wymaganie minimalne
Pomoc techniczna	Pomoc techniczna świadczona co najmniej w dni robocze w godzinach pracy Jednostki Zamawiającego.
Wymagania dotyczące dostarczanego oprogramowania	
Nowość i pochodzenie	Oprogramowanie nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania, nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) muszą być wolne od wad fizycznych i prawnych.

2. Platforma szkoleniowa z zakresu cyberbezpieczeństwa – 31 użytkowników, 12 miesięcy

Parametr / funkcja	Wymaganie minimalne
Postanowienia ogólne	
Przeznaczenie	Usługa podnoszenia świadomości bezpieczeństwa (Security Awareness Training) umożliwiająca prowadzenie kampanii edukacyjnych z zakresu podstaw bezpieczeństwa w Internecie, bezpieczeństwa informacji podczas pracy zdalnej oraz bezpieczeństwa IT w codziennych obowiązkach pracowników.
Liczba użytkowników	Dostęp do platformy dla co najmniej 31 użytkowników.
Okres świadczenia usługi	12 miesięcy od dnia udostępnienia platformy Zamawiającemu.
Dostęp do platformy	Platforma dostępna za pomocą dowolnej nowoczesnej przeglądarki internetowej (Chrome, Firefox, Edge).
Lokalizacja usługi	Usługa świadczona z centrum danych znajdującego się na terenie Unii Europejskiej.
Dostępność	Wszystkie moduły usługi świadczone w trybie 24/7/365.
Spójność rozwiązania	Wszystkie moduły (platforma zarządzająca, platforma szkoleniowa, platforma phishingowa, moduł raportowania, moduł quizów, moduł narzędzi dodatkowych) pochodzą od jednego producenta.
Język użytkownika	Przy tworzeniu konta użytkownika możliwy wybór domyślnego języka, w którym użytkownik otrzymuje powiadomienia i kampanie phishingowe oraz ma dostęp do szkoleń.
Platforma szkoleniowa	
Biblioteka szkoleń	Co najmniej 250 szkoleń dostępnych w 40 językach.
Materiały w języku polskim	Łączny czas trwania wszystkich materiałów szkoleniowych w języku polskim wynosi co najmniej 10 godzin.
Formy szkoleń	Szkolenia w postaci filmów, plików audio, prezentacji, broszur oraz interaktywnych gier, zakończone testami lub quizami sprawdzającymi przyswojenie przedstawionego materiału merytorycznego.
Zakres tematyczny	Szkolenia obejmują co najmniej następujące zagadnienia: a) ryzyko związane z AI, b) bezpieczeństwo informacji, c) klasyfikacja informacji, d) cykl życia informacji, e) własność intelektualna, f) hasła, g) kontrola dostępu, h) poczta e-mail, i) bezpieczeństwo w Internecie, j) inżynieria społeczna (socjotechnika), k) prywatność, l) dane płatnicze, m) phishing, n) malware, wirusy i ransomware, o) kradzież tożsamości, p) media społecznościowe, q) praca zdalna, r) urządzenia mobilne, s) wyciek danych, t) otwarte sieci Wi-Fi, u) usługi chmurowe, v) prywatne urządzenia w organizacji (BYOD), w) bezpieczeństwo w podróży.

Parametr / funkcja	Wymaganie minimalne
Tryby realizacji szkoleń	To samo szkolenie dostępne zarówno w trybie wymagającym interakcji (np. odtworzenia filmu w całości przed przejściem dalej), jak i w trybie przeglądu, który nie wymaga interakcji do ukończenia szkolenia.
Grupy użytkowników	Możliwość podziału użytkowników na grupy, dla których przygotowywane są indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.
Moduł quizów	
Quizy niezależne	Możliwość utworzenia quizu niezwiązanego z żadnym szkoleniem.
Udostępnianie quizów	Quizy dostępne w trzech formatach: ogólnodostępne, tylko dla wybranych użytkowników lub dostępne wyłącznie za pośrednictwem linku.
Zasady zaliczania	Administrator określa, czy zaliczenie quizu wymaga uzyskania określonej punktacji oraz czy quiz można powtarzać w przypadku niepowodzenia.
Pytania	Pytania do quizów tworzone ręcznie przez administratora lub pobierane z innych modułów systemu.
Moduł narzędzi dodatkowych	
Materiały uzupełniające	Grafiki, ulotki i animacje do wydruku lub umieszczenia w interaktywnych elementach infrastruktury Zamawiającego, np. animacja w stopce wiadomości e-mail informująca o zagrożeniach lub o prowadzonej kampanii edukacyjnej.
Platforma phishingowa	
Symulowane kampanie phishingowe	Generowanie i wysyłanie spreparowanych wiadomości phishingowych do wszystkich użytkowników usługi, w ich domyślnym języku.
Rodzaje wiadomości	Możliwość generowania co najmniej następujących typów wiadomości e-mail: a) z linkiem prowadzącym do strony internetowej, b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikacja, czy użytkownicy podadzą login i hasło na fałszywej stronie), przy zapewnieniu bezpieczeństwa takiej operacji przez platformę, c) z załącznikiem zawierającym potencjalnie niebezpieczny kod, d) z załącznikiem w postaci dokumentu Word, Excel, PowerPoint, PDF lub archiwum ZIP zawierającym potencjalnie niebezpieczny kod.
Reakcja na błąd użytkownika	Możliwość automatycznego skierowania użytkownika, który dał się oszukać, na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.
Rozłożenie wysyłki w czasie	Możliwość dystrybucji wiadomości phishingowych w czasie, tak aby nie wszyscy użytkownicy otrzymali tę samą wiadomość jednocześnie.
Baza szablonów	Rozbudowana baza szablonów wiadomości i stron phishingowych, obejmująca co najmniej wiadomości: a) Microsoft/Office 365, b) Microsoft Teams, c) Microsoft SharePoint, d) Microsoft OneDrive, e) DHL, f) o przekroczeniu limitu skrzynki pocztowej, g) Zoom, h) Google Drive, i) Apple.
Własne szablony	Możliwość wgrania własnego szablonu wiadomości e-mail.
Moduł raportujący	
Raport szkoleń	Status wykonania szkoleń przez użytkowników, z podziałem na grupy, z uwzględnieniem terminu wykonania szkoleń oraz wyników quizów i testów.

Parametr / funkcja	Wymaganie minimalne
Raport kampanii phishingowych	Status kampanii wraz z liczbą wysłanych wiadomości e-mail oraz szczegółami: kto otworzył wiadomość, kto i kiedy dał się oszukać, kto otworzył załącznik, kto wpisał dane w formularzu, z jakiej platformy i przeglądarki wykonano daną akcję, wraz ze szczegółowymi datami tych operacji.
Kampanie zintegrowane	
Łączenie modułów w kampanię	Szkolenia, quizy i symulacje phishingu mogą zostać połączone w jedną spójną kampanię, realizowaną krok po kroku według ustalonego wcześniej harmonogramu, bez konieczności interakcji z zewnątrz.