Gdańsk, dnia 11.01.2021 r.

Centralny nr postępowania: ZZ/ 41 /055/U/20

Dotyczy: postępowania o udzielenie zamówienia publicznego na audytu bezpieczeństwa platformy oraz infrastruktury IT w ramach projektu ,,MOST DANYCH. Multidyscyplinarny Otwarty System Transferu Wiedzy – etap II: Open Research Data"

Zamawiający – Politechnika Gdańska zawiadamia, że w przedmiotowym postępowaniu Wykonawca zgłosił pytania do treści ogłoszenia:

Testy penetracyjne aplikacji

1. Czy zakres prac obejmuje testy strony www (bez logowania do aplikacji)?
   Odpowiedź: Tak.

2. Prosimy o potwierdzenie, że zakres prac obejmuje tylko poniższe aplikacje:
   a. Aplikacja Most Wiedzy – Nauka (po zalogowaniu)
   b. Aplikacja Most Wiedzy – Biznes (po zalogowaniu)

   Odpowiedź : Nie. Obejmuje również strony MOST Wiedzy bez logowania (w tym w szczególności repozytorium otwartych danych badawczych) oraz dwa podsystemy dedykowane organizatorom konferencji naukowych oraz redakcjom czasopism naukowych (po zalogowaniu i bez).

W odniesieniu do aplikacji Most Wiedzy – Nauka (po zalogowaniu) prosimy o poniższe informacji:

3. Czy aplikacja będzie w pełni gotowa do testów? Czy też aplikacja podlega rozwojowi?
   Odpowiedź: Aplikacja cały czas podlega i będzie podlegać rozwojowi. Audytowany będzie zakres funkcjonalny systemu na moment rozpoczęcia audytu.
4. Czy funkcje będą gotowe do testów w obu aplikacjach i nie będą w czasie testów prowadzone żadne prace developerskie na testowanych wersjach aplikacji?
   Odpowiedź: Do ustalenia z Wykonawcą na etapie realizacji. Zamawiający dopuszcza możliwość, że na środowisku testowym przez określony czas nie będzie wgrywana nowa wersja oprogramowania.
5. Krótki opis do czego służy aplikacja oraz kluczowe funkcje (lista głównych funkcji).

   Odpowiedź: Jest to autorska platforma MOST Wiedzy wytworzona i rozwijana przez Centrum Usług Informatycznych Politechniki Gdańskiej, w tym w szczególności repozytorium otwartych danych badawczych. W skład platformy wchodzą również dwa moduły open source:

   https://pkp.sfu.ca/ojs/

   https://getindico.io/

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 14 63
fax: +48 58 347 14 90
e-mail: biuro.most@pg.edu.pl
http://pg.edu.pl/most

które zostały zintegrowane i zaadoptowane do potrzeb projektu.

Platforma promuje dorobek poszczególnych naukowców i potencjał jednostek naukowych. Zawiera Repozytorium Otwartych Danych Badawczych oraz system wspierający organizację konferencji naukowych (na bazie indico) i redaktorów czasopism naukowych (na bazie OJS).

6. Lista metod logowania i uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms)
   Odpowiedź: Zewnętrzny ID Provider przez protokół OAuth (3 różne). Moduły konferencji i czasopism zintegrowane z kontem w platformie.
7. Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token, kod sms, urządzenia HSM (Hardware Security Module)).
   Odpowiedź: ACL na podstawie uwierzytelnionego użytkownika.
8. Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np. administrator – zarządza prawami dostępu innych użytkowników).
   Odpowiedź: Zamawiający przewiduje kilkanaście ról, szczegółowa liczba zostanie określana etapie realizacji.
9. Lista / Orientacyjna liczba stron / podstron.
   Odpowiedź: Platforma obejmuje ok 70 ścieżek funkcyjnych.
10. Lista / Orientacyjna liczba formularzy (podstron, na której użytkownik może wprowadzać dane np. strona logowania, formularz kontaktowy, składanie zamówień itp.) dynamicznie generowanych.
    Odpowiedź: Około 70 formularzy.
11. Orientacyjna liczba pól we wszystkich formularzach.
    Odpowiedź: Kilkanaście do dwudziestu na formularz.
12. Szacunkowa (orientacyjna) liczba wszystkich używanych zmiennych (GET, POST, nagłówków - z uwzględnieniem ew. zmiennych przyjmowanych np. przez elementy Flash - jeśli występują) w całym testowanym systemie. Chodzi o sumaryczną / całkowitą liczę parametrów w całej aplikacji, która ma być przedmiotem testów.
    Odpowiedź: Zamawiający nie prowadzi takiej statystyki.

W odniesieniu do aplikacji Most Wiedzy – Biznes (po zalogowaniu) prosimy o poniższe informacje:

Odpowiedź: Odpowiedź została udzielona w pkt. 1 -12 powyżej (obejmuje również część biznesową platformy).

1. Czy aplikacja będzie w pełni gotowa do testów? Czy też aplikacja podlega rozwojowi?
2. Czy funkcje będą gotowe do testów w obu aplikacjach i nie będą w czasie testów prowadzone żadne prace developerskie na testowanych wersjach aplikacji?
3. Krótki opis do czego służy aplikacja oraz kluczowe funkcje (lista głównych funkcji).
4. Lista metod logowania i uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms).

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 14 63
fax: +48 58 347 14 90
e-mail: biuro.most@pg.edu.pl
http://pg.edu.pl/most

5. Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token, kod sms, urządzenia HSM (Hardware Security Module)).
6. Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np. administrator – zarządza prawami dostępu innych użytkowników).
7. Lista / Orientacyjna liczba stron / podstron.
   Lista / Orientacyjna liczba formularzy (podstron, na której użytkownik może wprowadzać dane np. strona logowania, formularz kontaktowy, składanie zamówień itp.) dynamicznie generowanych.
8. Orientacyjna liczba pól we wszystkich formularzach.
9. Szacunkowa (orientacyjna) liczba wszystkich używanych zmiennych (GET, POST, nagłówków - z uwzględnieniem ew. zmiennych przyjmowanych np. przez elementy Flash - jeśli występują) w całym testowanym systemie. Chodzi o sumaryczną / całkowitą liczę parametrów w całej aplikacji, która ma być przedmiotem testów.

Przegląd konfiguracji środowiska aplikacji

11. Serwery baz danych – prosimy informację o producencie i wersji poszczególnych komponentów (np. OS, serwer aplikacyjny), które mają być przebadane
12. Serwery www – prosimy informację o producencie i wersji poszczególnych komponentów (np. OS, serwer aplikacyjny), które mają być przebadane
13. Serwery aplikacji – prosimy informację o producencie i wersji poszczególnych komponentów (np. OS, serwer aplikacyjny), które mają być przebadane
14. Serwery PHP / Python – prosimy informację o producencie i wersji poszczególnych komponentów (np. OS, serwer aplikacyjny), które mają być przebadane
15. Serwery składowania danych – prosimy informację o producencie i wersji komponentów (np. OS, serwer aplikacyjny), które mają być przebadane

Odpowiedź 11-15: Zamawiający wykorzystuje technologię: nginx, postgresql, elastic search, spring, symfony, storage obiektowy zgodny z S3. Szczegóły stosu technologicznego zostaną przekazane na etapie audytu.

16. Prosimy o doprecyzowanie co dokładnie ma być wykonane i odniesieniu do jakich konkretnie komponentów infrastruktury w poniższym punkcie:
    - Ustawień systemów zabezpieczeń (w tym konfiguracji szyfrowanej transmisji danych) wykorzystywanych w ramach platformy MOST Wiedzy.

Odpowiedź: W ramach zadania Zamawiający wymaga wykonania weryfikacji konfiguracji poszczególnych serwerów aplikacji oraz połączeń sieciowych pomiędzy komponentami i z zewnątrz.

Przegląd infrastruktury IT

17. Prosimy o:
    a. Liczby urządzeń
    b. Producentów urządzeń

c. Wersji urządzeń

które mają być objęte testami penetracyjnymi urządzeń (wykonane przy pomocy narzędzi analizujących sieć)

18. Prosimy o:

    a. Nazwy serwera
    b. Producenta
    c. Wersji

19. W odniesieniu do punktu dotyczącego audytu serwerów (parametry sprzętowe, parametry programowe, konfiguracja, administracja zasobami, bezpieczeństwo danych i stosowanych zasad archiwizacji w tym tworzenia kopii zapasowych).

Odpowiedź 17-19: Platforma (kilkanaście podów) zlokalizowana jest w dwóch prywatnych chmurach obliczeniowych zbudowanych z wykorzystaniem rozwiązania Kubernetes oraz węzłów obliczeniowych w postaci maszyn wirtualnych w oparciu o OpenStack i VMWare działających pod kontrolą systemu operacyjnego klasy linux.

20. W odniesienie do punktu „Dodatkowo Wykonawca opracuje wytyczne w zakresie modernizacji i rozbudowy infrastruktury IT do poziomu spełniającego wymagania bezpieczeństwa wynikające z aktualnych przepisów prawa, dobrych praktyk branżowych i normy PN-ISO/IEC 27001:2014-12 (wytyczne do modernizacji: sieci teleinformatycznej, sprzętu komputerowego, serwerów, zarządzania i oprogramowania użytkowego) oraz wskaże obszary zmian dotyczące stosowanej lub brakującej dokumentacji (procedury, instrukcje), samej organizacji Centrum Usług Informatycznych i innych elementów, które mają lub mogą mieć wpływ na poziom bezpieczeństwa.", prosimy o:

    a. Informację jak szczegółowe mają być wytyczne?
    b. Kto będzie odbiorcą tych wytycznych?
    c. Specyfikację przepisów prawa, o które Zamawiający ma na myśli.
    d. Specyfikację dobrych praktyk, które Zamawiający ma na myśli.

Odpowiedź: Odbiorcą będzie zespół specjalistów Centrum Usług Informatycznych – projektantów (w tym DevOps) oraz administratorów. Poziom szczegółowości dostosowany do grupy odbiorców. Dotyczy przepisów prawa obowiązujące uczelnie wyższe jako jednostki administracji publicznej.

21. W celu wskazania brakującej dokumentacji, o której mowa w punkcie powyżej konieczne jest przeprowadzenie kompleksowego audytu bezpieczeństwa wszystkich regulacji i dokumentacji Zamawiającego wg ISO 27001. Czy Zamawiający oczekuje takiego kompleksowego audytu?

Odpowiedź: Nie.

<u>Opracowanie raportu końcowego</u>

22. W odniesieniu do punktu „poziom krytyczności błędu według zaproponowanej przez Wykonawcą i uzgodnionej z Zamawiającym klasyfikacją" czy Zamawiający akceptuje poniższą klasyfikację krytyczności błędu:

    a. Krytyczne
    b. Wysokie
    c. Średnie
    d. Niskie

Jeżeli nie to prosimy o wytyczne Zamawiającego odnośnie klasyfikacji krytyczności błędu.

Odpowiedź: Tak, przy czym należy opisać co się z tym wiąże mając na uwadze ryzyko i wpływ na organizację.

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 14 63
fax: +48 58 347 14 90
e-mail: biuro.most@pg.edu.pl
http://pg.edu.pl/most

23. Czy szkolenie może być przeprowadzone zdalnie?
Odpowiedź: Tak
24. Ile osób będzie uczestniczyć w szkoleniu?
Odpowiedź: Kilka – kilkanaście zależenie od charakteru wykrytych błędów.
25. Prosimy o zmianę daty przeniesienia praw autorskich – prawa autorskie zostaną przeniesione na Zamawiającego po zapłacie całości należnego Wykonawcy wynagrodzenia.
Odpowiedź:
Zamawiający zmienia treść §7 umowy – Prawa Autorskie. §7 wzoru umowy otrzymuje brzmienie:

1. *Wykonawca gwarantuje Zamawiającemu, że realizacja Umowy nie spowoduje naruszenia praw autorskich, znaków handlowych i towarowych, patentów, rozwiązań konstrukcyjnych, know-how i innych praw chronionych.*
2. *Wykonawca przejmuje na siebie wszelką odpowiedzialność za roszczenia osób trzecich w związku z realizacją Umowy, dotyczącą w szczególności naruszenia czyichkolwiek praw autorskich, znaków handlowych i towarowych, patentów, rozwiązań konstrukcyjnych, know-how oraz innych praw chronionych.*
3. *Zamawiający w ramach wynagrodzenia za wykonanie Przedmiotu Umowy, z chwilą odbioru końcowego przedmiotu umowy, nabywa majątkowe prawa autorskie do wszystkich utworów i własność do fizycznych egzemplarzy utworów, w rozumieniu ustawy o prawie autorskim i prawach pokrewnych, wykonanych przez Wykonawcę w ramach niniejszej umowy (w tym wszelkiej dokumentacji autorstwa Wykonawcy), na wszystkich znanych w chwili zawierania umowy polach eksploatacji, w tym: zwielokrotnianie; edytowanie; zmiany; utrwalanie; rozpowszechnianie, publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym; użyczenie i najem; publiczne wykonywanie; wyświetlanie; odtwarzanie; nadawanie w telewizji; wprowadzanie do obrotu w tym poprzez sieć Internet; wprowadzanie do pamięci komputera.*
4. *Wykonawca udziela Zamawiającemu zezwoleń do dokonywania wszelkich zmian i przeróbek utworów, o których mowa w ust. 3, osobiście lub za pośrednictwem osób trzecich, w tym również do wykorzystania ich w części lub całości oraz łączenia z innymi utworami.*
5. *Zamawiający ma prawo korzystać i rozpowszechniać utwory, o których mowa w ust. 3, a także ma prawo do ich opracowania bez oznaczania ich imieniem i nazwiskiem ich twórcy.*
6. *Zamawiający ma prawo przenieść prawa lub upoważnić osoby trzecie do korzystania z uzyskanych zezwoleń a także dokonywać w przekazanych utworach zmian osobiście lub za pośrednictwem osób trzecich.*
7. *Przez zezwolenia, o których mowa w ust. 6, rozumie się zezwolenia udzielone wyłącznie Zamawiającemu. Zezwolenia te są nieodwołalne i nie są uzależnione od żadnych warunków oraz zostały udzielone bez prawa wypowiedzenia lub cofnięcia.*
8. *Wykonawca oświadcza, że przy realizacji umowy będzie przestrzegał przepisów ustawy o prawie autorskim i prawach pokrewnych oraz nie naruszy praw majątkowych osób trzecich.*
9. *Wykonawca najpóźniej w dniu podpisania protokołu odbioru końcowego wyda Zamawiającemu również wystawione przez autora utworu nieodwołalne i bezwarunkowe upoważnienie dla Zamawiającego do wykonania w imieniu autora(ów) utworu(ów) – jego(ich) autorskich praw osobistych, a w szczególności do: decydowania o nienaruszalności treści i formy utworu, decydowania o pierwszym udostępnieniu dzieła publiczności, decydowania o nadzorze nad sposobem korzystania z utworu oraz wykonywania innych autorskich praw osobistych, jak również oświadczenie o zrzeczeniu się przez twórcę/ów wykonywania tych praw.*
10. *Przeniesienie praw określonych niniejszym paragrafem Umowy następuje bez ograniczeń czasowych i terytorialnych.*

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 14 63
fax: +48 58 347 14 90
e-mail: biuro.most@pg.edu.pl
http://pg.edu.pl/most

W związku z udzielnymi odpowiedziami i wprowadzonymi zmianami Zamawiający zmienia termin składania ofert z 12.01.2021 na 14.01.2021 r.

Odpowiedzi na pytania i zmiany stają się integralną częścią ogłoszenia i są wiążące dla wszystkich Wykonawców biorących udział w niniejszym postepowaniu.

Kanclerz
Politechniki Gdańskiej
mgr inż. Mariusz Miler

.....
(podpis kierownika Zamawiającego/ osoby upoważnionej)

MOST DANYCH

POLITECHNIKA GDAŃSKA

ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 14 63
fax: +48 58 347 14 90
e-mail: biuro.most@pg.edu.pl
http://pg.edu.pl/most