Załącznik nr 6 do SIWZ ZP/195/025/U/12
Załącznik nr 1 do umowy

Opis Przedmiotu Zamówienia na realizację audytów dla poszczególnych Inicjatyw i infrastruktury IT w ramach projektu eUczelnia

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

SPIS TREŚCI

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

A. Wstęp

Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu audytów oprogramowania dla poszczególnych usług w ramach projektu eUczelnia. Projekt jest finansowany z UE w ramach Regionalnego Programu Operacyjnego dla Województwa Pomorskiego na lata 2007-2013 – działanie 2.2.2. Szczegółowe informacje dotyczące projektu dostępne są na stronie www.euczelnia.pg.gda.pl.

B. Wymagania wstępne przed realizacją audytu

Wykonawca przed przystąpieniem do realizacji audytu jest zobowiązany do podpisania klauzuli poufności i jest zobligowany do zachowania w tajemnicy wszelkich informacji pozyskanych w sposób bezpośredni lub pośredni dotyczących Zamawiającego, a w szczególności danych osobowych, technicznych, ekonomicznych lub organizacyjnych.

Zobowiązanie do zachowania poufności dotyczy wszelkich informacji udzielonych ustnie, pisemnie, drogą elektroniczną lub w inny sposób w odpowiedzi na zapytania Wykonawcy w trakcie realizacji zadań audytowych i jest bezterminowe.

C. Obszary prac audytowych

Przewiduje się realizację wymienionych w poniższych tabelach (tab. 1, tab. 2) obszarów audytowych:

Obszar I. Audyt oprogramowania
Audyt 1. Oprogramowanie świadczące usługi z obszaru eDziekanat.
Audyt 2. Oprogramowanie świadczące usługi z obszaru eStudent.
Audyt 3. Oprogramowanie świadczące usługi z obszaru eRekrutacja
Audyt 4. Oprogramowanie świadczące usługi z obszaru eNauka.
Audyt 5. Oprogramowanie świadczące usługi z obszaru eWspółpraca.
Audyt 6. Oprogramowanie świadczące usługi z obszaru eArchiwum.
Audyt 7. Oprogramowanie świadczące usługi z obszaru eKontakt.
Audyt 8. Oprogramowanie świadczące usługi z obszaru eNauczanie.

Tabela 1. Audyt oprogramowania.

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

Obszar II. Audyt Infrastruktury IT.
Audyt 9. eKręgosłup - Zakupiona w ramach projektu infrastruktura teleinformatyczna.

Tabela 2. Audyt konfiguracji infrastruktury IT.

D. Harmonogram realizacji audytów

Proponowany Harmonogram realizacji audytów został przestawiony w poniższej tabeli.

Harmonogram realizacji audytów	
Audyt 1 – eDziekanat	**1 miesiąc od dnia podpisania umowy**
Audyt 2 – eStudent	**02.07.2012**
Audyt 3 – eRekrutacja	**01.09.2013**
Audyt 4 – eNauka	**03.06.2013**
Audyt 5 – eWspółpraca	**02.12.2013**
Audyt 6 – eArchiwum	**01.01.2013**
Audyt 7 – eKontakt	**03.09.2012**
Audyt 8 – eNauczanie	**01.04.2013**
Audyt 9 – eKręgosłup	**01.10.2013**

Tabela 3. Harmonogram realizacji audytów.

Powyższy harmonogram (tab. 3) nie jest ostateczny. Zamawiający zastrzega sobie prawo wyznaczenia terminów realizacji poszczególnych audytów z 30 dniowym wyprzedzeniem uwzględniając aktualny poziom zaawansowania prac nad poszczególnym obszarem.

Dodatkowo zakłada się, że w przypadku przedstawienia Zamawiającemu rekomendacji wdrożenia zmian, które zostaną wprowadzone w środowisku produkcyjnym Wykonawca wykona testy regresyjne po uzgodnieniu z Zamawiającym terminu ich wykonania. Termin ich zakończenia nie może być jednak dłuższy niż 30 dni po zgłoszeniu do Wykonawcy wprowadzenia poprawki wykrytych błędów w środowisku produkcyjnym.

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

E. Szczegółowy zakres audytu oprogramowania

W obszarze I *„Audyt oprogramowania”*, Zamawiający wskazuje, że wybrane aplikacje osadzone są na tej samej platformie, stanowiącej środowisko konfiguracyjne dla nowych produktów.

Zakres merytoryczny musi objąć następujące zadania:

Zakres prac.
Zadanie I. Przeprowadzenie audytu dokumentacji dla obszarów objętych działaniem oprogramowania określającego zgodność z normą PN-ISO/IEC 27001:2007.
Zadanie II. Przeprowadzenie testów penetracyjnych aplikacji.
Zadanie III. Przegląd konfiguracji środowiska aplikacji.
Zadanie IV. Opracowanie raportu końcowego.
Zadanie V. Przeprowadzenie testów regresyjnych w przypadku wykrycia istotnych błędów pod względem istotności i prawdopodobieństwa ich wystąpienia.

Tabela 4. Zakres prac audytowych do wykonania w ramach obszaru I.

Szczegółowe wymagania zawarte w tabeli 4 zostały przedstawione poniżej.

Zadanie I. Przeprowadzenie audytu dokumentacji dla obszarów objętych działaniem oprogramowania określającego zgodność z normą PN-ISO/IEC 27001:2007.

Wykonawca zobowiązany będzie do przeanalizowania i oceny wytworzonych w projekcie dokumentów pod kątem stosowania zasad i dobrych praktyk w odniesieniu do systemu zarządzania bezpieczeństwem informacji w tym, m.in.: Polityki Bezpieczeństwa Informacji, Planów Zachowania Ciągłości Działania dla stworzonych i opracowywanych aplikacji oraz innych dokumentów związanych z bezpieczeństwem i rekomendacji poprzednio realizowanych prac w obszarze zwiększenia poziomu bezpieczeństwa.

Wykonawca dokona weryfikacji posiadanej przez Zamawiającego dokumentacji w odniesieniu do wymogów normy PN-ISO/IEC 27001:2007. Weryfikacji podlegać będą m.in.: zakres merytoryczny dokumentów i ich aktualność w tym określenie

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

zakresu koniecznych zmian związanych z wymogami normy PN-ISO/IEC 27001:2007. W ramach zadnia przeanalizowane mają być, m.in.:

- Wyniki przeprowadzonych prac związanych z bezpieczeństwem (m.in.: polityka bezpieczeństwa czy plany zachowania ciągłości działania),
- Aktualnie stosowane polityki, procedury i inne dokumenty związane z bezpieczeństwem (np. istniejące zapisy, uregulowania itp.).

Wykonawca uwzględni wytyczne przedstawione w Załączniku A normy PN-ISO/IEC 27001:2007 a w szczególności:

- **A.7 -** Zarządzanie Aktywami.
- **A.9** - Bezpieczeństwo Fizyczne i Środowiskowe.
- **A.10** - Zarządzanie Systemami i Sieciami.
- **A.11** - Kontrola Dostępu.
- **A.12** - Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.
- **A.13** - Zarządzanie incydentami związanymi z bezpieczeństwem informacji i słabości.
- **A.14** - Zarządzanie ciągłością działania.
- **A.15** - Zgodność.

W ramach realizacji audytu Wykonawca przeprowadzi identyfikację powiązań między obszarami, które są wspierane przez aplikacje stworzone przez Zamawiającego z innymi obszarami bądź podmiotami zewnętrznymi.

Działanie to obejmować ma również określenie, m.in.: rodzaj zasobów wykorzystywanych w działaniach w danym obszarze oraz obszarach powiązanych takich jak: systemy i infrastruktura techniczna, ludzie, zbiory przetwarzanych informacji oraz procedury działania (spisane i nieformalne).

Identyfikacja ta ma zostać przeprowadzona na podstawie dokumentacji z tego zakresu jak również na bazie badania ankietowego wśród pracowników Zamawiającego oraz wywiadów bezpośrednich. Badanie ankietowe oraz wywiady bezpośrednie obejmą około 25 pracowników.

W ramach pracy Wykonawca opracuje wnioski audytowe oraz rekomendacje dalszych działań i koniecznych zmian odnoszących się do zapewnienia zgodności działania zbudowanych aplikacji z wymaganiami normy PN-ISO/IEC 27001:2007 i najlepszymi praktykami w dziedzinie zarządzania np. ITIL. Wnioski te będą stanowiły część końcowego raportu z audytu.

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

Zadanie II. Przeprowadzenie testów penetracyjnych aplikacji.

Sposób realizacji Testów Penetracyjnych będzie realizowany przez Wykonawcę w następujący sposób:

a. Analiza systemu, konfiguracji dostępnych usług oraz dokumentacji systemu pod kątem identyfikacji potencjalnych zagrożeń i opracowanie wykazu obszarów tych zagrożeń.
b. Inwentaryzacja rzeczywistych zasobów systemu, obejmująca: zasoby sprzętowe, softwarowe oraz obszar transmisji danych (wykorzystywane porty, media, protokoły komunikacyjne, etc.) i opracowanie raportu inwentaryzacyjnego.
c. Przygotowanie metodologii planowanych testów penetracyjnych (rodzaj testu, narzędzie, harmonogram) wraz z ich uzasadnieniem. Metodyka musi pokrywać zagrożenia potencjalne, jak i zagrożenia zidentyfikowane na podstawie inwentaryzacji rzeczywistego systemu. Przy projektowaniu zakresu testów należy uwzględnić najnowsze opracowania (zawierające listy krytycznych aspektów bezpieczeństwa systemów, listy najczęściej występujących podatności, kategoryzacji typów ataków, itp.) organizacji zajmujących się bezpieczeństwem teleinformatycznym (SANS, OISSG, OWASP, NIST, CERT, NASK).
d. Testy systemu zgodnie z opracowaną metodyką:
    - z poziomu sieci Internet,
    - z poziomu sieci bezprzewodowej,
    - z poziomu sieci lokalnej.
e. Sporządzenie raportu z wykonanych testów, analiza wyników oraz przedstawienie rekomendacji minimalizujących zagrożenia, o ile takie zostały wykryte (*wymaganie szerzej opisane w pkt. Zadanie V. Opracowanie raportu zaleceń audytowych*).

Testy penetracyjne powinny odbyć się dla szeregu scenariuszy testowych:

- Użytkownik nieposiadający konta w aplikacji.
- Użytkownik posiadający w aplikacji konto o standardowych (obniżonych) uprawnieniach.
- Użytkownik posiadający w aplikacji konto administratora, ale nieposiadający uprawnień do serwera, na którym jest hostowana aplikacja.

Dodatkowo, Wykonawca w ramach umowy, po wprowadzeniu przez Zamawiającego poprawek do wykrytych błędów podczas testów, przeprowadzi jedną iterację ponownych testów wskazanych przypadków testowych w zakresie zaraportowanych błędów oraz zweryfikuje, czy wykryte przez niego błędy zostały wyeliminowane i czy w związku z ich wprowadzeniem nie pojawiły się nowe problemy, widoczne bezpośrednio w trakcie powtarzania zgłoszonego przypadku testowego.

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

Zadanie III. Przegląd konfiguracji środowiska aplikacji.

Wykonawca zobowiązany będzie do przeprowadzenia przeglądu platformy, o ile aplikacja powiązana z usługą jest na niej osadzona oraz do konfiguracji środowiska aplikacji, w szczególności do:

- Konfiguracji serwerów baz danych wykorzystywanych w ramach systemu eUczelnia.
- Konfiguracji serwerów WWW wykorzystywanych w ramach systemu eUczelnia.
- Konfiguracji systemów operacyjnych wykorzystywanych w ramach systemu eUczelnia,
- Ustawień systemów zabezpieczeń (w tym konfiguracji szyfrowanej transmisji danych) wykorzystywanych w ramach systemu eUczelnia.

Konfiguracja środowiska ma zostać przebadana pod kątem zgodności z aktualnym stanem wiedzy zakresie bezpieczeństwa IT dla zastosowanych rozwiązań. Dodatkowo, tam gdzie jest to możliwe, Wykonawca odniesie się do opublikowanych zaleceń dotyczących konfiguracji aplikacji lub systemów w przyszłości, tak aby projektowane nowe rozwiązania informatyczne uwzględniały przedstawione rekomendacje w zakresie bezpieczeństwa.

Zadanie IV. Opracowanie raportu końcowego.

Wykonawca zobowiązany będzie do przedstawienia szczegółowego raportu z wykonanych prac. Raport zawierać musi informacje o przebiegu badania, znalezionych błędach oraz zalecenia poaudytowe. Raporty końcowe zawierające podsumowanie wykonanych prac, dostarczane są Zamawiającemu po zakończeniu każdego audytu z obszarów I i II. Raporty obejmować muszą przynajmniej informacje wymienione poniżej:

- poziom krytyczności błędu według zaproponowanej przez Wykonawcą i uzgodnionej z Zamawiającym klasyfikacją,
- prawdopodobieństwo znalezienia/wykorzystania podatności przez atakującego – tzw. Likehood,*probability*,
- wpływ na system (lub inne systemy) – tzw. *impact*,
- szczegółowy sposób wykrycia i charakterystyka ataku (z uwzględnieniem zasad

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

powtarzalności dla każdego przypadku). Informacje powinny być na tyle szczegółowe, aby była możliwa reprodukcja danego błędu,

- możliwości zabezpieczenia się przed podatnością i uwagi prowadzące do uniknięcia tego typu problemów w przyszłości,
- załączniki dokumentujące wystąpienie błędu (np. zrzuty ekranu, przykładowe pakiety atakujące lub świadczące o podatności, pliki zawierające zapis ruchu sieciowego w formacie *libpcap* itp.).

Wykonawca jest zobligowany do opracowania następujących definicji:

- kryterium wpływu na systemu (impact),
- prawdopodobieństwo wykorzystania podatności przez atakującego (likelihood),
- poziom krytyczności

oraz przedstawienia Zamawiającemu do akceptacji sposobu prezentacji wyników audytu. Zamawiający oczekuje, że dla wykrytych błędów o wpływie na system: średni lub krytyczny i równoczesnym prawdopodobieństwie: średni lub wysoki zostaną opracowane przez Wykonawcę szczegółowe rekomendacje zmian.

Struktura raportu powinna odpowiadać merytorycznemu podziałowi prac na obszary i aplikacje. Dodatkowo należy uwzględnić podział logiczny struktury aplikacji na następujące warstwy:

- baza danych,
- warstwa dostępu do bazy,
- warstwa biznesowa,
- warstwa prezentacji,
- warstwa bezpieczeństwa.

Ponadto Wykonawca będzie zobowiązany do prezentacji wyników audytu po każdym z nich w formie 2-godzinnego szkolenia oraz przeprowadzenia prezentacji wyników zadań I-III w formie 8-godzinnego szkolenia dla programistów systemu i administratorów środowiska, pozwalającego na zapoznanie się z wykrytymi błędami oraz na uzyskanie wiedzy w zakresie ich unikania.

Wykonawca, z dniem podpisania protokołu odbioru raportu, przenosi na Zamawiającego autorskie prawa majątkowe do raportu na polach eksploatacji, obejmujących:

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

- odtwarzanie,
- utrwalanie i trwałe zwielokrotnianie całości lub części utworu, wszystkimi znanymi w chwili zawierania Umowy technikami, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową,
- przekazywanie,
- przechowywanie,
- wyświetlanie,
- wprowadzanie do pamięci komputera wraz z prawem do dokonywania modyfikacji,
- tłumaczenie,
- przystosowywanie,
- zmiany układu lub jakiekolwiek inne zmiany,

F. Szczegółowy zakres audytu infrastruktury IT

W ramach niniejszego zadania należy przeprowadzić następujące prace:

Audyt infrastruktury informatycznej:

- Audyt systemów wykorzystywanych w ramach systemu eUczelnia dostępnych z sieci Internet.
- Audyt systemów wykorzystywanych w ramach systemu eUczelnia dostępnych z sieci LAN.
- Audyt urządzeń aktywnych wykorzystywanych w ramach systemu eUczelnia.
- Audyt konfiguracji serwerów wykorzystywanych w ramach systemu eUczelnia.

Zakres audytu infrastruktury informatycznej:

Testy penetracyjne urządzeń (wykonane przy pomocy narzędzi analizujących sieć) będą obejmować m.in.:

- Badanie portów sieciowych celem wykrycia potencjalnych luk bezpieczeństwa w dostępnych usługach.
- Analizę odporności na ataki typu „denial of service”.
- Użycie przez Wykonawcę narzędzi eksploatujących wykryte luki bezpieczeństwa.
- Analizę środowiska sieciowego (skanowanie, dekodowanie, analiza protokołów i pakietów w sieci, statystyki ruchu sieciowego, przykładowa

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl

ewidencja zdarzeń sieciowych, przegląd topologii sieci, systemów operacyjnych pod kątem sieciowym).

- Analizę aktualności oprogramowania urządzeń (firmware), wygenerowanie listy wszystkich koniecznych uaktualnień oprogramowania.
- Audyt polegający na wykryciu oprogramowania typu Spyware.
- Audyt serwerów (parametry sprzętowe, parametry programowe, konfiguracja, administracja zasobami, bezpieczeństwo danych i stosowanych zasad archiwizacji).
- Audyt min. 10% stacji roboczych i terminali (parametry sprzętowe, parametry programowe, konfiguracji, administracja zasobami, monitoring zasobów).

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 (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.

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

Biuro Projektu
tel.(058) 348 63 84
www.euczelnia.pg.gda.pl