Protokół z wyboru oferty
dotyczącej zapytania ofertowego z dnia 10 czerwca 2013 r. na wdrożenie wybranych wymagań normy PN-ISO/IEC 27001:2007 w ramach projektu „Nowoczesne zarządzanie Wyższą Szkołą Informatyki Stosowanej i Zarządzania”

1. **Zamawiający:**

Wyższa Szkoła Informatyki Stosowanej i Zarządzania
ul. Newelska 6,
01-447 Warszawa
tel. 22 455 80 00
Fax: 22 34 86 501
e-mail: wit@wit.edu.pl

2. **Przedmiot zamówienia**

Wspólny słownik zamówień:
72224200-3 - usługi w zakresie planowania zapewnienia jakości systemu
79417000-0 - usługi doradcze w zakresie bezpieczeństwa
72263000-6 - usługi wdrażania oprogramowania

Uaktualnienie polityki bezpieczeństwa informacji

W związku z realizacją projektu „Nowoczesne zarządzanie Wyższą Szkołą Informatyki Stosowanej i Zarządzania” uczelnia realizuje wdrożenie wybranych wymagań normy PN-ISO/IEC 27001:2007 w celu zapewnienia bezpieczeństwa informacji.

3.1. Opis zamówienia

3.1.1. Uaktualnienie obecnie funkcjonującej Polityki Bezpieczeństwa Informacji w WSISIZ, rozumianej jako spójny zbiór dokumentów określających reguły i sposoby postępowania niezbędne do zapewnienia poufności, integralności i dostępności informacji przetwarzanych w WSISIZ, w oparciu o wytyczne normy PN-ISO/IEC 27001:2007 (System Zarządzania Bezpieczeństwem Informacji) oraz z uwzględnieniem obszaru danych osobowych (zapewnienie zgodności WSISIZ z wymaganiami Ustawy o ochronie danych osobowych i aktów wykonawczych).

3.1.2. Przeprowadzenie testów bezpieczeństwa obejmujących testy penetracyjne typu black-box dwóch aplikacji webowych oraz analiza podatności pięciu serwerów.

3.2. Procedura wykonania

3.2.1. Dokumentacja Polityki Bezpieczeństwa Informacji w WSISIZ

Zamawiający oczekuje od Wykonawcy opracowania dokumentacji, której zakres powinien być adekwatny do sklasyfikowanych informacji przetwarzanych w WSISIZ. Zamawiający posiada zidentyfikowane informacje sklasyfikowane jako dane osobowe oraz jako tajemnica przedsiębiorstwa.

W szczególności dokumentacja musi uwzględniać następujący zakres zagadnień:

a) dotyczący informacji:

- Klasyfikacja informacji, w tym informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu obowiązujących przepisów prawa (tj. Ustawy o ochronie danych osobowych, oraz Ustawy o zwalczaniu nieuczciwej konkurencji),
- Polityka Bezpieczeństwa Informacji WSISIZ (wymagania bezpieczeństwa dla WSISIZ, z uwzględnieniem szczególnych przepisów prawa, które mają zastosowanie w WSISIZ – dokument ogólny),
- Polityka Bezpieczeństwa (w rozumieniu rozporządzenia MSWiA z dn. 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych),
- Zakres odpowiedzialności Użytkownika Systemu WSISIZ,
- Zakres odpowiedzialności Administratora Systemu WSISIZ
- Procedura zarządzania incydentami bezpieczeństwa
- Nadzór nad dokumentacją,
- Nadzór nad zapisami,
- Audyt wewnętrzny,

b) dotyczący systemu przetwarzania:

- Instrukcja zarządzania systemem informatycznym (zgodnie z wymaganiami Rozporządzenia MSWiA z dn. 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych)
- Procedura wprowadzania zmian w systemach przetwarzania WSISIZ,
- Procedura zarządzania elementami uwierzytelniającymi,
- Procedura awaryjnego pobrania elementów uwierzytelniających,
- Procedura nadawania/odbioru uprawnień w systemach WSISIZ,
- Procedura dostępu stron trzecich do systemów WSISIZ,
- Procedura postępowania w przypadkach naruszenia bezpieczeństwa systemów WSISIZ,
- Procedura obsługi awarii w WSISIZ,
- Instrukcja postępowania w przypadkach awaryjnych,
- Procedura tworzenia i przechowywania kopii zapasowych,

- Procedura niszczenia nośników informacji,
- Wytyczne do zarządzania ciągłością działania

Wykonawca zaproponuje strukturę dokumentacji odwzorowującą wszystkie określone wyżej zagadnienia oraz określającą hierarchię zależności (powiązań) dokumentów między sobą. Dopuszcza się, by Wykonawca w ramach opracowanej przez siebie struktury dokumentacji zaproponował własne tytuły dokumentów inne, niż wymienione w punktach a) i b) powyżej, a także by zagadnienia wymienione w punktach a) i b) powyżej były grupowane i opisywane łącznie we wspólnych dokumentach, o ile logika przyjętej przez Wykonawcę koncepcji takie podejście uzasadnia. Wykonawca zaproponuje także jednolity szablon dla dokumentów.

3.2.2. Przetwarzanie danych osobowych z ustawą

W ramach zapewnienia zgodność WSISIZ z wymaganiami Ustawy o ochronie danych osobowych Wykonawca wykona:

- analizę istniejących zbiorów danych osobowych pod kątem legalności przetwarzania danych osobowych oraz możliwości ich ewentualnego zintegrowania,

3.3. Testy bezpieczeństwa

Wykonawca przedstawi metodykę wg której wykona testy bezpieczeństwa. Po jej akceptacji Wykonawca przeprowadzi testy, sporządzi raport z testów zawierający co najmniej: wyniki prac, ich analizę, ocenę krytyczności wykrytych luk i podatności oraz rekomendacje mające na celu minimalizację ryzyk wynikających z tych podatności i luk. Zamawiający nie dopuszcza możliwości dostarczenia przez Wykonawcę raportów wygenerowanych bezpośrednio z narzędzi do testów bezpieczeństwa. Wymagana jest co najmniej manualna weryfikacja wyników pochodzących z tychże narzędzi to testów oraz własna ocena wpływu wykrytych podatności na bezpieczeństwo testowanych zasobów.

3.4. Wymagania na zespół mający realizować prace

- Doświadczenie we wdrażaniu i utrzymaniu systemów zarządzania bezpieczeństwem informacji zgodnych z wymaganiami normy ISO 27001
- Doświadczenie we wdrażaniu i utrzymaniu systemów zarządzania ciągłością działania
- Posiadanie udokumentowanych uprawnień do audytowania systemów zarządzania bezpieczeństwem informacji oraz ciągłością działania
- Doświadczenie w zakresie wdrażania i utrzymania dokumentacji danych osobowych wymaganej przepisami prawa lub doświadczenie, co najmniej w zakresie sprawowania nadzoru nad przetwarzaniem danych osobowych.
- Doświadczenie w realizacji testów bezpieczeństwa systemów teleinformatycznych
- Kompetencje w zakresie znajomości metod i technik badania podatności w systemach teleinformatycznych oraz ich zabezpieczania przed atakami, udokumentowane międzynarodowymi certyfikatami branżowymi.

Wiedza osób, członków zespołu, powinna być potwierdzona następującymi certyfikatami:

- CISSP (Certified Information Systems Security Professional),
- CISM (Certified Information Security Manager),
- Audytor wiodący systemu ISO 27001,
- PRINCE2TM Practitioner

lub certyfikatami równoważnymi.

3. Sposób upublicznienia zapytania ofertowego

Zapytanie ofertowe zostało zamieszczone w dniu 10 czerwca 2013 r. na stronie internetowej zamawiającego www.wit.edu.pl oraz zostało wysłane drogą elektroniczną za potwierdzeniem odbioru do następujących potencjalnych Wykonawców:

I. PBSG Sp. z o.o.

ul. Skotarska 8
61-625 Poznań
e-mail: marta.markiewicz@pbsg.pl

II. Centrum Doradztwa w Informatyce i Zarządzaniu Sp. z o.o.

ul. Mogilska 25
31-542 Kraków
e-mail: Krzysztof.Atlasiewicz@cediz.pl

III. MERITUM – Doradztwo i Szkolenia Sp. z o.o.

ul. Jutrzenki 116
02-230 Warszawa
e-mail: m.karas@meritum.biz.pl

IV. DECSOFT S.A.

ul. Kolejowa 5/7
01-217 Warszawa
e-mail: krzysztof.gierkowski@decsoft.com.pl

4. Tryb udzielenia zamówienia

Proces wyboru Wykonawcy przeprowadzono w oparciu o zasadę przejrzystej i uczciwej konkurencji, która obowiązuje podmioty realizujące projekty w ramach Programu Operacyjnego Kapitał Ludzki, które z mocy obowiązujących przepisów prawa nie są zobowiązane do stosowania ustawy Prawo Zamówień Publicznych.

5. Kryterium oceny ofert:

Cena – waga 60 % , doświadczenie 40 %

6. Otwarcie ofert

Otwarcie ofert odbyło się 21 czerwca 2013 r. w Biurze Projektu w siedzibie Zamawiającego. Do upłynięcia terminu przewidzianego w zapytaniu ofertowym, tj. 21 czerwca 2013 r. do godziny 12:00 złożone zostały 4 (cztery) oferty przez:

- BLUE energy Sp. z o.o.
ul. Towarowa 35
61-896 Poznań – data wpływu 20 czerwca 2013 r.

- PBSG Sp. z o.o.
ul. Skotarska 8
61-625 Poznań – data wpływu 20 czerwca 2013 r.

- MERITUM – Doradztwo i Szkolenia Sp. z o.o.
ul. Jutrzenki 116
02-230 Warszawa – data wpływu 20 czerwca 2013 r.

- DECSOFT S.A.
ul. Kolejowa 5/7
01-217 Warszawa – data wpływu 21 czerwca 2013 r.

7. Informacja o spełnianiu warunków udziału w postępowaniu

Oferenci spełnili wymagane warunki udziału w postępowaniu

8. Wykonawcy wykluczeni

Nie dotyczy

9. Oferty odrzucone

Nie dotyczy

10. Wybór oferty

Komisja w następującym składzie:

Bartłomiej Solarz-Niesłuchowski – przewodniczący komisji
Anna Piotrowska - członek komisji
Marzena Osuch - członek komisji
Albina Miler - członek komisji
Maciej Mikita - członek komisji

wybrała ofertę złożoną przez MERITUM – Doradztwo i Szkolenia Sp. z o.o.
ul. Jutrzenki 116
02-230 Warszawa
Cena: 19 926,00 zł (słownie: dziewiętnaście tysięcy dziewięćset dwadzieścia sześć zł, 0 gr.)
punktacja **97,60**.

Oceny komisji kształtowały się w sposób następujący:

			A	B	C	D	E	średnia średnich	kwota
BLUE energy Sp. z o.o.	kryt. 1	60%	62,79	62,79	62,79	62,79	62,79	62,79	31 734,00
	kryt. 2	40%	80,00	70,00	80,00	90,00	70,00		
	średnia "ważona"		69,67	65,67	69,67	73,67	65,67	68,87	
PBSG Sp. z o.o.	kryt. 1	60%	53,11	53,11	53,11	53,11	53,11	53,11	37 515,00
	kryt. 2	40%	100,00	90,00	100,00	90,00	100,00		
	średnia "ważona"		71,87	67,87	71,87	67,87	71,87	70,27	
MERITUM – Doradztwo i Szkolenia Sp. z o.o.	kryt. 1	60%	100,00	100,00	100,00	100,00	100,00	100,00	19 926,00
	kryt. 2	40%	85,00	90,00	95,00	100,00	100,00		
	średnia "ważona"		94,00	96,00	98,00	100,00	100,00	**97,60**	
DECSOFT S.A.	kryt. 1	60%	32,34	32,34	32,34	32,34	32,34	32,34	61 623,00
	kryt. 2	40%	95,00	100,00	100,00	95,00	90,00		
	średnia "ważona"		57,40	59,40	59,40	57,40	55,40	57,80	

11. Uzasadnienie dokonanego wyboru

Oferta odpowiada wymaganiom określonym w specyfikacji istotnych warunków zamówienia zamieszczonej na stronie zamawiającego i została oceniona jako najkorzystniejsza w oparciu o przyjęte kryteria.