Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Usługa certyfikacji działu IT Uczelni na zgodność z normą ISO/IEC 27001:2022 lub równoważną* wraz z nadzorem nad skutecznością działania systemu jakości

Katolicki Uniwersytet Lubelski Jana Pawła II (dalej również KUL) wdrożył w wybranym zakresie wymagania normy ISO/IEC 27001:2022 (zwaną dalej Normą) i na potwierdzenie skuteczności podjętych działań w zakresie bezpieczeństwa poszukuje niezależnej jednostki certyfikacyjnej, która potwierdzi skuteczność opracowanego Systemu Zarządzania Bezpieczeństwem Informacji (dalej również SZBI) zgodnie z przywołaną Normą lub normą równoważną. Posiadanie certyfikacji na zgodność z Normą pozwoli KUL na:

1) spełnienie przez Zamawiającego formalnych wymogów Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247).
2) Poprawę efektywności działania procedur,
3) Realne podniesienie poziomu bezpieczeństwa KUL,
4) Budowanie wizerunku KUL w zakresie bezpieczeństwa i innowacyjności

Preambuła

Intencją Zamawiającego jest potwierdzenie skuteczności działania SZBI oraz uzyskanie niezależnej opinii o stopniu wdrożenia wymagań Normy czego potwierdzeniem ma być uzyskanie certyfikatu.

1. Zamawiający określił zakres certyfikacji, dla lokalizacji podstawowej jako: *Zarządzanie procesami wspierającymi utrzymanie i rozwój systemów informatycznych pionu IT, w zakresie sieci wewnętrznej KUL*
2. Zamawiający określił zakres certyfikacji, dla lokalizacji dodatkowej jako: *Tworzenie, przechowywanie, utrzymanie kopii zapasowych systemów informatycznych KUL*
3. Zamawiający planuje objąć zakresem certyfikacji 25 osób, pracujących w trybie jednozmianowym, w pełnym wymiarze etatu, w dwóch lokalizacjach
4. Zamawiający nie korzysta z podwykonawców, wykonujących prace na systemach w jego imieniu. Utrzymaniem i rozwojem systemów zajmuje się własna kadra informatyczna.
5. Zamawiający nie zidentyfikował skomplikowanych procesów, lub systemów. Zamawiający nie wykorzystuje systemów chmurowych w zakresie certyfikacji.
6. Na dzień opracowywania Opisu Przedmiotu Zamówienia, Deklaracja Stosowania, wymagana do procesu certyfikacji posiadała status „w opracowaniu".

Wymagany zakres czynności od Wykonawcy to przynajmniej:

1. Wykonawca przeprowadzi audyt certyfikujący i dwa audyty nadzoru.

2. Wykonawca uwzględni w wycenie i zrealizuje wszystkie niezbędne działania konieczne do podjęcia w ramach audytu certyfikacyjnego oraz audytów nadzoru.
3. Zakres prac audytowych obejmuje:
   a) analizę istniejących u Zamawiającego dokumentów, w tym m. in. Polityki Bezpieczeństwa, procedur, instrukcji, regulaminów dotyczących bezpieczeństwa informacji, wchodzących w skład SZBI;
   b) ocenę ww. dokumentów pod kątem zgodności z normą ISO/IEC 27001:2022 lub równoważną, w oparciu o Załącznik A tej normy lub wykazy załączone do norm równoważnych;
   c) weryfikację poprawności wdrożenia i funkcjonowania opisanych zabezpieczeń;
   d) weryfikację poprawności realizacji procedur, zawartych w Politykach Bezpieczeństwa;
   e) opracowanie raportu z audytu zawierającego opis skuteczności funkcjonowania SZBI w odniesieniu do kryteriów oceny zawartych w Normie;
   f) sformułowanie niezgodności i rekomendacji.
4. Audyty nadzoru powinny odbyć się przed upływem 12 miesięcy od dnia decyzji o certyfikacji. Nadzór drugi – przed upływem 12 miesięcy od dnia wykonania pierwszego audytu nadzoru.
5. Po przeprowadzeniu całego procesu audytu certyfikującego, Wykonawca przekaże raport z audytu w terminie 70 dni od dnia podpisania umowy, Raport powinien zawierać co najmniej:
   a) cel i zakres (obszary) audytu,
   b) stosowaną normę,
   c) opis metodyki audytu,
   d) imiona i nazwiska audytorów,
   e) opis przeprowadzonych prac,
   f) ustalenia (próbki) oraz dowody tych ustaleń,
   g) ocenę spełniania wymagań zgodnie z klasyfikacją Wykonawcy (np. zgodność/niezgodność/punkt do doskonalenia/spostrzeżenie/częściowa zgodność),
   h) sformułowane niezgodności wraz ze wskazaniem punktów normy, w których te niezgodności występują,
6. Audyt powinien być przeprowadzony w siedzibie Zamawiającego. Za zgodą wyrażoną przez Zamawiającego dopuszcza się możliwość przeprowadzenia audytu w formie zdalnej. W przypadku audytowania online, Wykonawca powinien zapewnić narzędzie do komunikacji również dla pracowników Zamawiającego.

Wymagania w zakresie dostarczonej dokumentacji

1. Dokumenty przekazywane przez Wykonawcę powinny posiadać ujednoliconą czcionkę;
2. Dokumentację – o ile ma to zastosowanie - należy zasadniczo sporządzać w formacie A4;
3. W miarę możliwości schematy, rysunki i mapy należy zamieszczać wewnątrz dokumentów;
4. Dokumentację należy sporządzać w języku polskim;
5. Dokumentacja dostarczona elektronicznie powinna być przekazywana w formatach obsługiwanych co najmniej przez pakiety Libre Office, Microsoft Office bądź Acrobat Reader;

6. Dokumentację należy dostarczyć w wersji elektronicznej w sposób uzgodniony z Zamawiającym;
7. Zamawiający ma prawo do jednej tury zgłaszania uwag do przekazywanego raportu w terminie 14 dni od daty przekazania Raportu z audytu, do których Wykonawca powinien się odnieść w ciągu kolejnych 14 dni.

Wymagania dla Wykonawcy:

1. O przeprowadzenie audytu certyfikującego może ubiegać się Jednostka certyfikująca posiadająca, bądź ubiegająca się o akredytację w zakresie certyfikacji na zgodność z ISO 27001:2022 lub równoważnej*
2. Wykonawca posiada co najmniej trzech czynnych Audytorów wiodących.

Uwagi do umowy:

1. Terminy realizacji: proces certyfikacji powinien zakończyć się nie później niż w ciągu 70 dni od dnia podpisania umowy. Za dni robocze rozumie się dni przypadające od poniedziałku od piątku, z wyłączeniem dni ustawowo wolnych od pracy.
2. Niezbędna jest umowa powierzenia danych osobowych - powinna ona uwzględniać usunięcie wszystkich danych roboczych po zakończeniu świadczenia usługi oraz ich bezpieczeństwo w trakcie przetwarzania.
3. Wszelka komunikacja (wymiana dokumentów) między Wykonawcą a kadrą Wykonawcy dotycząca usługi, realizowana będzie za pośrednictwem środków komunikacji określonych lub zaakceptowanych przez Zamawiającego.
4. Zamawiający dopuszcza audytowanie w formie zdalnej, przy wykorzystaniu komunikatorów on-line. W przypadku audytowania online, Wykonawca powinien zapewnić narzędzie do komunikacji również dla pracowników Zamawiającego.

Wspólny Słownik Zamówień (CPV):

(CPV): 72224200 - Usługi w zakresie planowania zapewniania jakości systemu

****Opis równoważności:***

1. W przypadku, kiedy Wykonawca oferować będzie certyfikację i wdrożenie normy innej niż norma ISO/IEC 27001 ocenie podlegać będzie odpowiedniość proponowanej do realizacji normy do przygotowania Zamawiającego do opracowania i ustanawiania, wdrażania i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI zapewniającym poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2. W szczególności certyfikacja i wdrożenie zaleceń równoważnej normy zapewniać ma:

   1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;

3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;

6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

a) zagrożenia bezpieczeństwa informacji,

b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

a) monitorowanie dostępu do informacji,

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności

technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

3. Równoważna norma musi zapewniać analogiczne uprawnienia do normy ISO/IEC 27001 wskazane w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 - § 20. ust. 1.