OGŁOSZENIE

Wydział Informatyki Urzędu Miasta w Ostrowcu Świętokrzyskim
zaprasza firmy do składania ofert na:

„Przeprowadzenie audytu bezpieczeństwa przetwarzania informacji oraz opracowanie i wdrożenie systemu bezpieczeństwa przetwarzania informacji w Systemie Informatycznym Urzędu Miasta w Ostrowcu Świętokrzyskim"

I. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Cel zamówienia.

1.1. Weryfikacja spełnienia przez systemy teleinformatyczne Zamawiającego wymagań określonych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwanym dalej Rozporządzeniem

1.2. Opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji i systemu zarządzania usługami IT, wskazanych w Rozporządzeniu, w wymaganiach dla systemów teleinformatycznych.

Analiza systemów IT pod kątem bezpieczeństwa dostępu do danych i przechowywania danych w formie elektronicznej oraz wykonanie raportu wraz z zaleceniami dotyczącymi procedur ochrony informacji elektronicznej wykonanych w oparciu o:

- Normę PN-ISO/IEC 27001 „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania"
- Normę PN-ISO/IEC 17799 „Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji"
- Normę PN-ISO/IEC 27005 „Technika informatyczna - Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji"
- Normę PN-ISO/IEC 24762 „Technika informatyczna - Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie"
- Normę PN-ISO/IEC 20000-1 „Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja"
- Normę PN-ISO/IEC 20000-2 „Technika informatyczna - Zarządzanie usługami – Część 2: Reguły postępowania"
- Ustawę o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jednolity z 2014r., poz.1182),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiada urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
- Ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005r. (Dz. U. 2005 nr 64, poz. 565 z późniejszymi zmianami)
- Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań

dla systemów teleinformatycznych z dnia 12 kwietnia 2012 r. (Dz.U z 2012 r. nr 526), zwane dalej Rozporządzeniem

- Ustawę o ochronie informacji niejawnych z dnia 5 sierpnia 2010 (Dz.U. z 2010 nr 182, poz.1228)
- Ustawę o dostępie do informacji publicznej z dnia 6 września 2001 roku (Dz.U. z 2001 nr 112, poz.1198 z późniejszymi zmianami)

1.3. Dostarczenie raportu oraz dokumentacji zawierającej wykaz czynności, wykonanie których pozwoli na uzyskanie zgodności stanu faktycznego zabezpieczeń z zaleceniami zawartymi w w/w Rozporządzeniu, w odniesieniu do systemów teleinformatycznych Zamawiającego i określającej dalsze prace związane z wdrożeniem systemu zarządzania bezpieczeństwem informacji.

1.4 Dostarczenie raportu odnośnie dostosowania serwerowni Miejskiego Systemu Informatycznego w lokalizacji przy ul. Świętokrzyskiej 22 w Ostrowcu Świętokrzyskim, do wymagań zgodnych z normą ISO 27001.

1.5. Szkolenie dla pracowników Zamawiającego z zakresu zasad zarządzania bezpieczeństwem informacji

2. Szczegółowy zakres prac

Dostosowanie systemów teleinformatycznych Zamawiającego do wymagań określonych w Rozporządzeniu obejmuje:

2.1. Analizę systemów teleinformatycznych Zamawiającego pod kątem:

- Formatu zapisu danych
- Sposobu kodowania znaków
- Formatów i protokołów wymiany danych
- Zgodności z wymaganiami Web Content Accessibility Guidelines 2.0 dla systemów służących do prezentacji zasobów informacji

2.2. Opracowanie i wdrożenie systemów zarządzania bezpieczeństwem informacji (lub danych) obejmujące:

1) Formalne zdefiniowanie zakresu systemów zarządzania bezpieczeństwem informacji (lub danych)

- Określenie obszaru funkcjonowania Zamawiającego, w którym systemy te zostaną wdrożone. Określenie zakresu powinno bazować na analizie funkcjonowania Zamawiającego i wymaganiach wynikających z przepisów prawnych.

2) Analiza ryzyka

- Zdefiniowanie procesu zarządzania ryzykiem
- Inwentaryzację aktywów informacyjnych
- Identyfikację podatności
- Ocenę ryzyka
- Opracowanie planu postępowania z ryzykiem

3) Zdefiniowanie zasad eksploatacji systemów zarządzania

- Określenie deklaracji stosowania obejmującej wykaz zabezpieczeń wymienionych w załączniku A normy PN-ISO/IEC 27001, cele ich stosowania, a także zabezpieczenia z załącznika A, które nie będą stosowane.
- Określenie polityk systemów zarządzania bezpieczeństwem informacji. Polityki mają zawierać deklaracje kadry zarządzającej dotyczące zarządzania bezpieczeństwem informacji i zarządzania usługami.
- Określenie i sformalizowanie zasad zarządzania przetwarzaniem informacji poprzez osoby odpowiedzialne za przetwarzanie informacji oraz wskazanie podejścia do zapewnienia zasobów niezbędnych do efektywnego zarządzania bezpieczeństwem i zarządzania usługami.
- Określenie zasad monitorowania efektywności systemów zarządzania.
- Określenie zasad przeprowadzania wewnętrznych i zewnętrznych audytów, w szczególności poprzez wskazanie częstotliwości audytów, sposobu przygotowywania i zatwierdzania ich planów, sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników.
- Określenie zasad wprowadzania działań korygujących w przypadku niezgodności z wymaganiami systemów zarządzania. W szczególności zasady te będą określać zdarzenia mogące zainicjować określenie i wprowadzenie działania korygującego, sposób analizy niezgodności i identyfikowania działań korygujących, sposób ich wprowadzania i dokumentowania, przegląd ich realizacji.
- Określenie zasad wprowadzania działań zapobiegawczych w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemów zarządzania. W szczególności zasady te będą określać zdarzenia mogące zainicjować określenie i wprowadzenie działań zapobiegawczych, sposób analizy zidentyfikowanych problemów i określanie działań zapobiegawczych, sposób ich wprowadzania, dokumentowania, przegląd ich realizacji.
- Określenie zasad przeglądów systemów zarządzania bezpieczeństwem danych (informacji), w szczególności określenie częstotliwość przeglądów, zakres i sposób ich przeprowadzania, materiały źródłowe niezbędne do przeprowadzenia przeglądu, tryb wdrażania wniosków.
- Określenie zasad nadzoru nad dokumentami wchodzącymi w skład systemów zarządzania, w szczególności określenie zasady wersjonowania, zatwierdzania, dystrybucji, przechowywania, archiwizowania i niszczenia dokumentów. Także określenie zasady przechowywania, archiwizowania oraz niszczenia zapisów (rejestrów).

4) Opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji

- Optymalizacja posiadanych przez Zamawiającego dokumentów określających zasady zarządzania bezpieczeństwem informacji.
- Opracowanie dokumentów określających zasady zarządzania bezpieczeństwem informacji, których brak stwierdzono po przeprowadzeniu analizy ryzyka

W opracowaniu maja być wzięte pod uwagę następujące zagadnienia:

- Wymagania w zakresie zabezpieczeń technicznych.
- Zasady bezpiecznego przetwarzania informacji przez pracowników Zamawiającego.
- Zasady klasyfikacji informacji.

- Zasady zarządzania dostępem do informacji.
- Zasady publikacji informacji.
- Zasady wymiany danych z podmiotami zewnętrznymi.
- Zasady wymiany danych wewnątrz Urzędu.
- Zasady wprowadzania zmian w przetwarzaniu informacji, w szczególności z wykorzystaniem systemów informatycznych.
- Wytyczne w zakresie utrzymania dokumentacji zabezpieczeń i systemów informatycznych
- Zasady zgłaszania podatności w mechanizmach przetwarzających informacje.
- Wymagania dot. sposobu usuwania podatności.
- Zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa informacji.
- Zasady kontroli bezpieczeństwa informacji.
- Zasady zarządzania oprogramowaniem.
- Zasady zarządzania kopiami zapasowymi.
- Zasady konserwacji i serwisu zabezpieczeń technicznych i systemów informatycznych.
- Zasady monitorowania bezpieczeństwa infrastruktury informatycznej.
- Zasady przygotowania urządzeń IT do. użytkowania w systemie przetwarzania informacji zgodnie z wymaganiami bezpieczeństwa
- Zasady wycofywania urządzeń IT z użycia.
- Zasady użytkowania i niszczenia wymiennych nośników danych
- Wytyczne w zakresie ochrony fizycznej i technicznej dostępu do danych oraz pomieszczeń i urządzeń związanych z przetwarzaniem informacji
- Wytyczne w zakresie monitorowania przepisów prawnych związanych z ochroną informacji.
- Wytyczne w zakresie bezpiecznej współpracy z podmiotami zewnętrznymi.
- Wytyczne w zakresie bezpiecznego świadczenia usług związanych z przetwarzaniem informacji.
- Opracowanie dokumentów w zakresie ciągłości działania.
    - Strategia ciągłości przetwarzania informacji.
    - Ogólny plan ciągłości działania dla sytuacji uniemożliwienia przetwarzania informacji w systemach informatycznych.
    - Zasady przeglądu i aktualizacji planu.
    - Zasady testowania planu ciągłości działania.

5) Opracowanie i wdrożenie systemu zarządzania usługami na podstawie normy PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2 (zgodnie z §15 Rozporządzenia)

Dokumentacja ma definiować następujące procesy:

- Projektowania i wdrażania nowych lub zmodyfikowanych usług
- Zarządzania poziomem usług
- Raportowania usług
- Zarządzania dostępnością usług

- Zapewnienia ciągłości świadczenia usług
- Budżetowania i rozliczania usług
- Zarządzania pojemnością
- Zarządzania relacjami
- Zarządzania incydentami
- Zarządzania problemami
- Zarządzania konfiguracją
- Zarządzania wersjami oprogramowania?

2.3. Opracowanie dokumentacji wymaganej do bezpiecznego przetwarzania informacji (w tym danych osobowych):

- Aktualizacja istniejącej instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i dostosowanie jej do potrzeb Miejskiego Systemu Informatycznego obejmującego wiele lokalizacji w tym nową serwerownię
- Aktualizacja istniejącej polityki bezpieczeństwa przetwarzania danych osobowych i dostosowanie jej do potrzeb Miejskiego Systemu Informatycznego obejmującego wiele lokalizacji w tym nową serwerownię.

3. Zakres Audytu Bezpieczeństwa Informacji.

Audyt Bezpieczeństwa Informacji powinien obejmować następujące audyty:
3.1. Audyt zarządzania bezpieczeństwem danych osobowych, którego celem jest weryfikacja realizacji przez Zamawiającego czynności wymaganych w związku z przetwarzaniem danych osobowych zgodnie z Ustawą o Ochronie Danych Osobowych. Audyt powinien obejmować:

1) Analizę posiadanej przez Zamawiającego dokumentacji związanej z przetwarzaniem danych osobowych
2) Weryfikacja realizacji przez Administratora Bezpieczeństwa Informacji wymaganych czynności
3) Weryfikacja czynności związanych z upoważnianiem do przetwarzania danych osobowych
4) Weryfikacja poprawności powierzania przetwarzania danych osobowych

3.2. Audyt socjotechniczny, którego celem jest weryfikacja zagrożeń spowodowanych czynnikiem ludzkim. W ramach tego audytu należy przeprowadzić następujące testy:

- Próba uzyskania dostępu do komputera;
- Próba uzyskania dostępu do informacji;
- Symulacja umieszczenia szkodliwego oprogramowania na komputerze użytkownika;
- Sprawdzenie „odporności" użytkowników na ataki socjotechniczne z wykorzystaniem takich narzędzi jak: telefon, poczta elektroniczna, przenośna pamięć masowa (nie tylko zawarta na typowych urządzeniach typu „pendrive", ale też zawarta w aparatach fotograficznych i telefonach komórkowych);

- W szczególności sprawdzenie scenariuszy socjotechnicznych opartych o wysłanie fałszywego maila imitującego wiadomość służbową lub wykonywanie fałszywego telefonu

3.3. Audyt fizyczny i środowiskowy, którego celem jest weryfikacja skutecznej ochrony fizycznej i środowiskowej zasobów. Audyt ten powinien obejmować:

1) Weryfikację granic obszaru bezpiecznego
2) Weryfikację zabezpieczeń wejścia/wyjścia
3) Weryfikację systemów zabezpieczeń pomieszczeń i urządzeń
4) Weryfikację bezpieczeństwa okablowania strukturalnego
5) Weryfikację systemów chłodzenia
6) Weryfikację systemów alarmowych

3.4. Audyt teleinformatyczny, którego celem jest wykrycie potencjalnych zagrożeń związanych z utratą informacji w systemach informatycznych. Zakres audytu:

1) Weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi
2) Weryfikacja ochrony przed oprogramowaniem szkodliwym;
3) Weryfikacja procedur zarządzania kopiami zapasowymi;
4) Weryfikacja procedur związanych z rejestracją błędów;
5) Weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
6) Przeprowadzenie testów penetracyjnych przeprowadzonych ze stacji roboczej podłączonej do systemu informatycznego z zewnątrz (poprzez urządzenie łączące system informatyczny Urzędu z Internetem) mających na celu zidentyfikowanie podatności na włamanie;
7) Przeprowadzenie testów penetracyjnych przeprowadzonych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji,
8) Wykonanie testów penetracyjnych zarówno wewnętrznych (stacja robocza, ale też połączenie VPN) jak i zewnętrznych (prowadzonych przez Wykonawcę ze wskazanego przez niego adresu IP);
9) Weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe;
10) Weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania);
11) Identyfikację podatności systemów i sieci na wszystkie ataki typu: sniffing, spoofing, Man-in-the-Middle.
12) Identyfikację podatności systemów i sieci na ataki takie jak sniffing, spoofing, man-in-the-middle;
13) Weryfikacja otwartości portów i ocena związanych z tym ryzyk;
14) Weryfikacja rodzaju i wersji wykorzystywanego oprogramowania systemowego i usługowego - w tym obecność najnowszych poprawek bezpieczeństwa;
15) Weryfikacja rodzaju i wersji wykorzystywanego oprogramowania urządzeń (tzw. firmware)
16) Analiza i ocena mechanizmów zarządzania aktualizacjami;

17) Weryfikacja uruchomionych usług i procesów;
18) Weryfikacja podatności hostów na ataki w warstwie systemowej (przy wykorzystaniu exploitów);
19) Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego dostępu do zasobów plikowych;
20) Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego zdalnego (przez WWW) dostępu do paneli administracyjnych serwerów;
21) Analiza zastosowanych metod uwierzytelniania;
22) Weryfikacja obecności domyślnych kont użytkowników;
23) Weryfikacja mechanizmów logowania zdarzeń;
24) Analiza i ocena sposobu obsługi błędów;
25) Analiza i ocena dodatkowych systemów bezpieczeństwa tj. oprogramowania antywirusowego, oprogramowania weryfikującego integralność danych.

3.5. Analiza bezpieczeństwa systemu poczty elektronicznej obejmująca:

1) Analizę i ocenę konfiguracji oprogramowania filtrującego niechcianą pocztę elektroniczną;
2) Badanie podatności systemu na próby nieautoryzowanego dostępu do skrzynek poczty elektronicznej pracowników;
3) Badanie podatności systemu na próby podszycia się pod innych użytkowników poczty elektronicznej;
4) Badanie podatności systemu na próby rozsyłania niechcianej poczty elektronicznej;
5) Badanie podatności systemu na zakłócenie i/lub przerwanie ciągłości działania.

3.6. Analiza bezpieczeństwa usługi katalogowej Active Directory obejmująca:

1) Weryfikację polityk bezpieczeństwa (w tym polityki haseł) i weryfikacja ich poprawnego wymuszania na stacjach roboczych
2) Weryfikację bezpieczeństwa transmisji danych pomiędzy serwerem a stacjami roboczymi
3) Weryfikację reakcji i czasu reakcji na atak account lockout w domenie
4) Weryfikację skryptów logowania pod kątem ujawniania krytycznych informacji i wycieku danych

3.6. Wykonanie raportu z audytu, który będzie zawierał:

1) Cel i zakres audytu
2) Opis źródeł informacji wykorzystanych podczas przeprowadzania audytu
3) Ocenę zabezpieczeń i rekomendowane działania korekcyjne

4. Szkolenia pracowników Zamawiającego

Szkolenie pracowników zamawiającego powinno składać się z następujących szkoleń

1) Szkolenie pracowników Zamawiającego będących użytkownikami Systemu Informatycznego obejmujące następującą tematykę:
    - Omówienie podstawowych zasad bezpieczeństwa informacji i wypełniania procedur bezpieczeństwa informacji.
    - Zagrożenia związane z przetwarzaniem informacji.
    - Odpowiedzialność za naruszenie zasad bezpieczeństwa informacji.

- Zasady zgłaszania i procedury reagowania na incydenty.

2) Szkolenie pracowników Zamawiającego odpowiedzialnych za procedury bezpieczeństwa przetwarzania informacji w ilości 7 osób obejmujące tematykę:
   - Zagrożenia związane z przetwarzaniem informacji
   - Wymagania prawne związane z ochroną przetwarzanych informacji
   - Zasady bezpiecznego przetwarzania informacji
   - Zasady zarządzania bezpieczeństwem informacji
   - Zagrożenia związane z przetwarzaniem informacji
   - Odpowiedzialność za naruszenie zasad Polityki Bezpieczeństwa;
   - Zasady zgłaszania i procedury reagowania na incydenty.
   - Raportowanie incydentów i podatności związanych z ochroną informacji
   - Obowiązki pracowników w trakcie audytów systemów zarządzania
   - Konsekwencje nieprzestrzegania zasad bezpiecznego przetwarzania informacji

Wykonawca przekaże Zamawiającemu materiały szkoleniowe i prezentacje z przeprowadzonych szkoleń.

II. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW

1. Wiedza i doświadczenie

Wykonawca zobowiązany jest wykazać, się w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeśli okres prowadzenia działalności jest krótszy - w tym okresie (w przypadku świadczeń okresowych lub ciągłych uwzględniane są również zamówienia nadal wykonywane), należycie wykonał co najmniej:

2 zamówienia o wartości co najmniej 12 000,00 zł brutto każde z zamówień, polegających na wykonaniu testów penetracyjnych systemów teleinformatycznych;

2 zamówienia o wartości co najmniej 50 000,00 zł brutto każde z zamówień, polegające na przeprowadzeniu na wdrożeniu lub audytu systemu bezpieczeństwa informatycznego zgodnie ze standardem ISO 27001 lub Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

2. Osoby zdolne do wykonania zamówienia

Wykonawca zobowiązany jest wykazać, że dysponuje lub będzie dysponowało zespołem składającym się co najmniej z 3 osób i przynajmniej audytor wiodący legitymuje się wszystkimi niżej wymienionymi certyfikatami:

Audytor Wiodący ISO 27001;

Certified Information Systems Security Professional (CISSP) lub równoważny poświadczający posiadaną wiedzę z zakresu: kontroli dostępu, łączności i bezpieczeństwa sieci, zarządzania bezpieczeństwem informacji i zarządzania ryzykiem, bezpieczeństwa rozwoju aplikacji, kryptografii, architektury i projektowania pod kątem bezpieczeństwa, ciągłości działania i planowania odtworzenia w przypadku katastrofy, prawa, regulacji, czynności dochodzeniowych i zgodności z wymaganiami, bezpieczeństwa fizycznego.
Certified in Risk and Information Systems Control (CRISC) lub równoważny poświadczający posiadaną wiedzę z zakresu: identyfikacji, monitorowania i zarządzania ryzykiem IT oraz opracowywania, wdrażania i utrzymywanie mechanizmów kontrolnych w systemach informatycznych.
Certified Forensic Computer Examiner (CFCE) lub równoważny poświadczający kompetencje w dziedzinie informatyki śledczej.

Wykonawca zobowiązany jest wykazać, że posiada wdrożoną Politykę bezpieczeństwa oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zgodnie z przepisami ustawy o ochronie danych osobowych oraz Rozporządzeniem MSWiA z dnia 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 (Dz. U. z 2004 r. Nr 100, poz.1024).

Termin realizacji zamówienia: nie później niż **do dn. 31.03.2015 r.**
Planowane dwuetapowe wykonanie prac: I etap do 15.12.2014r. oraz II etap do 31.03.2015r.

3. Dodatkowe informacje na temat zakresu zamówienia można uzyskać w:
Urzędzie Miasta Ostrowca Świętokrzyskiego
Wydział Informatyki w godz. 7.30-15.30 pod nr tel.:
w sprawach formalnych Edyta Orłowska: 41/26 72 236
w sprawach technicznych Ferdynand Jagiełło: 41/26 72 135.

Cena ofertowa netto nie może przekroczyć równowartości 30 000 EURO brutto.
Oferty mogą podlegać negocjacjom w dół w zakresie ceny.
Oferent powinien mieć zarejestrowaną działalność gospodarczą.
Oferty zawierające proponowaną cenę, podstawowe dane firmy w tym numery:
REGON, NIP i datę rejestracji należy składać w Wydziale Informatyki Urzędu Miasta, pokój 131 w terminie do dnia 21.11 2014 roku do godz. 9^{00}.
Oferty mogą być składane również faxem i e-mailem:
fax: (0-41) 26 72 110
e-mail: wi@um.ostrowiec.pl

Zamawiający zastrzega sobie prawo unieważnienia zapytania ofertowego w każdym czasie bez podania przyczyny.

W przypadku przesyłania ofert za pośrednictwem poczty, ofertę należy kierować na adres:
Urząd Miasta, Wydział Informatyki, 27-400 Ostrowiec Świętokrzyski, ul. Głogowskiego 3/5.

Ostrowiec Św. dn. 14.11.2014 r.

Sekretarz Miasta
SEKRETARZ MIASTA
Ostrowca Świętokrzyskiego
mgr Marzena Dębniak