Załącznik nr 1 do projektu umowy

OPIS PRZEDMIOTU ZAMÓWIENIA

Audyt bezpieczeństwa Systemu URBANCARD Wrocławska Karta Miejska

Audytowi bezpieczeństwa podlegać będą wszystkie elementy infrastrukturalne składające się na całość rozwiązania Systemu URBANCARD Wrocławska Karta Miejska tj. serwery, serwery aplikacji, aplikacje, serwery bazodanowe, urządzenia końcowe, ruch sieciowy, systemy operatorskie.

W ramach umowy Wykonawca opracuje harmonogram oraz przedstawi raport z audytu.

Raport i omówienie wyników audytu nastąpi w miejscu wskazanym przez Zamawiającego.

Miejsce audytu: Warszawa, Wrocław

Zakres Audytu:

I. SYSTEMY OPERACYJNE

Weryfikacja prawidłowości instalacji i parametryzacji systemów operacyjnych w kontekście zapewnienie odpowiedniego poziomu bezpieczeństwa.

Zakres obejmuje w szczególności weryfikację:

- podziału przestrzeni dyskowej,
- udostępnionych usług sieciowych,
- implementacji procesów aktualizacji,
- implementacji systemu kopii zapasowych,
- systemów do logowania zdarzeń,
- mechanizmów administracji zdalnej,
- przypisania użytkowników do właściwych grup,

II. BAZY DANYCH

Weryfikacja prawidłowości instalacji i parametryzacji używanego RDBMS w kontekście zapewnienie odpowiedniego poziomu bezpieczeństwa i dostępności przechowywanych danych.

Zakres obejmuje w szczególności weryfikację i analizę:

- sposobu udostępniania RDBMS na poziomie sieciowym,
- zaimplementowanych systemów kopii zapasowych,

• implementacji podstawowych zasad hardeningowych bazy danych (np. logowanie zdarzeń, składowanie logów, partycjonowanie bazy, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL.),

• architektury bazy danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, wykorzystywanie widoków, wykorzystywanie procedur składowych, przechowywanie oraz dostęp do danych osobowych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych),

• analizę komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych).

• implementacji procesu aktualizacji.

III. APLIKACJE

Weryfikacja prawidłowości implementacji aplikacji systemu centralnego ze szczególnym uwzględnieniem elementów bezpośrednio wpływających na poziom bezpieczeństwa i stabilność systemu.

Zakres obejmuje w szczególności weryfikację i analizę:

• inspekcję mechanizmów uwierzytelniania / autoryzacji,

• obsługi błędów,

• poziomu bezpieczeństwa oferowanego przez aplikację,

• implementacji procesu aktualizacji.

IV. SIEĆ

Weryfikacja zasad utrzymania sieci, architektury i bezpieczeństwa.

Zakres obejmuje w szczególności analizę:

- weryfikacja topologii/architektury sieci.
- określenie usług działających w wybranych podsieciach,
- weryfikacja zasad utrzymania sieci,
- testy szczelności systemów klasy firewall,
- weryfikacja dostępnych portów i usług z Internetu.

V. Weryfikacja testów penetracyjnych

Weryfikacja zdolności podmiotu do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.

Weryfikacja kompletności dokumentacji. Weryfikacja wyników wykonanych testów penetracyjnych w oparciu o metodyki:

- OWASP TOP 10 (Open Web Application Security Project TOP 10 vulnerabilities)

- W zakresie: bezpieczeństwa aplikacji webowych

- W zakresie bezpieczeństwa aplikacji mobilnych: Top 10 Mobile Risks,

OWASP ASVS (Application Security Verification Standard Project)

- W zakresie: bezpieczeństwa aplikacji webowych (testy blackbox),

- W zakresie: ogólnego prowadzenia prac audytowych

VI. Zgodność z obowiązującymi Planem Ciągłości Działania Systemu oraz Politykami Bezpieczeństwa Systemu

• sprawdzenie dokumentacji w zakresie polityk bezpieczeństwa oraz Planów Ciągłości Działania Systemu URBANCARD Wrocławska Karta Miejska.
• weryfikacja kompletności dostarczonej dokumentacji, wywiad z osobami zaangażowanymi.

VII. Zgodność z obowiązującymi przepisami bezpieczeństwa danych osobowych i Polityk Bezpieczeństwa

Zakres obejmuje:

• sprawdzenie zgodności Systemu pod kątem obowiązujących rozporządzeń Parlamentu Europejskiego i Rady nr 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (inaczej ogólne rozporządzenie o ochronie danych osobowych - RODO),
• sprawdzenie zgodności Systemu pod kątem obowiązujących Polityk Bezpieczeństwa przetwarzania danych w Systemie oraz na urządzeniach końcowych,
• sprawdzenie procedur bezpieczeństwa dostępów podmiotów zewnętrznych,
• wypełnienie ankiety dotyczącej ochrony danych osobowych stanowiącej załącznik do zakresu audytu:

L.p.	PYTANIE	TAK/NIE DODATKOWE WYJAŚNIENIA
WIEDZA FACHOWA		
1.	Czy podmiot przetwarzający posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie? Czy udokumentowane?	
2.	Czy przepisy prawa wymagają, aby dany podmiot przetwarzający wyznaczył IOD?	
3.	Czy dany podmiot przetwarzający wyznaczył IOD? (Jeśli tak, proszę o przekazanie informacji kontaktowych do IOD)	
4.	Czy podmiot przetwarzający wyznaczył inną osobę/zespół odpowiedzialny za nadzór nad ochroną	

	danych osobowych w organizacji?	
5.	Czy osoby po stronie podmiotu przetwarzającego dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane z przepisami o ochronie danych? Czy jest to udokumentowane?	
6.	Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały przeszkolone w zakresie obsługi, w tym bezpiecznego korzystania z systemu informatycznego, jeżeli jest on stosowany do przetwarzania danych przez podmiot przetwarzający?	
7.	Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały przeszkolone w zakresie zasad bezpieczeństwa informacji?	
WIARYGODNOŚĆ		
8.	Czy podmiot przetwarzający posiada referencje od innych podmiotów, które obsługuje/obsługiwał w zakresie przetwarzania danych osobowych na ich zlecenie? Jeśli tak, czy można się z nią zapoznać?	
9.	Czy stwierdzono prawomocną decyzją UODO/innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający?	
10.	Czy podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów postępowania?	
11.	Czy podmiot przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący?	
12.	Czy podmiot przetwarzający otrzymał certyfikat zgodności z RODO?	
13.	Kryterium wewnętrzne: Czy rozważany podmiot jest znany na rynku jako podmiot wykonujący danego rodzaju usługi? Jeżeli tak, jaką ma renomę? Jakie są opinie o tym podmiocie, o współpracy z tym podmiotem, o stosowanych przez niego zabezpieczeniach czy przetwarzaniu danych?	
ZASOBY		
14.	Czy podmiot przetwarzający opracował i wdrożył politykę ochrony danych lub podobną procedurę? Jeśli tak, prosimy o jej przedstawienie.	
15.	Czy podmiot przetwarzających wdrożył procedurę/instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?	
16.	Czy podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych?	
17.	Czy podmiot przetwarzający prowadzi rejestr przetwarzanych zbiorów danych osobowych lub	

	zasobów informacyjnych ?	
18.	Czy podmiot przetwarzający prowadzi rejestry czynności przetwarzania danych osobowych (jako ADO oraz jako procesor)?	
19.	Czy podmiot przetwarzający wdrożył zasady zarządzania bezpieczeństwem informacji, w tym:	
19a.	system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001? Czy posiada certyfikat?	
19b.	zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002?	
19c.	zasady zarządzania bezpieczeństwem informacji zgodne z wymaganiami Krajowych Ram Interoperacyjności?	
20.	Czy podmiot wdrożył inne zasady ochrony informacji – (np. Polityka bezpieczeństwa informacji, Polityki ochrony danych osobowych, które są jego wewnętrznymi regulacjami)?	
20a.	Czy podmiot wdrożył inne zasady ochrony informacji – (Ramy prywatności, Praktyczne zasady ochrony informacji o identyfikowalnych osobach, Wytyczne dotyczące oceny skutków dla prywatności, itp.)?	
20b.	Czy podmiot wdrożył inne zasady, standardy, regulaminy, procedury, polityki, biblioteki lub zbiory najlepszych praktyk mające znaczenie dla ochrony informacji/danych osobowych?	
21.	Czy podmiot przetwarzający dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? (na podstawie szacowania ryzyka pod kątem ochrony prywatności - DPIA)?	
22.	Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania?	
23.	Czy podmiot przetwarzający okresowo przeprowadza kolejne działania związane z szacowaniem ryzyka pod kątem ochrony prywatności? Czy w przypadku zmiany poziomu ryzyka dobiera nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy?	
24.	Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym:	
a)	pseudonimizację i szyfrowanie danych,	
b)	zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów	

	i usług przetwarzania,	
c)	zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.	
25.	Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?	
26.	Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym?	
27.	Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych?	
28.	Czy osoby delegowane do obsługi ADO posiadają nadane upoważnienia do przetwarzania danych? Czy zostało to udokumentowane? Prosimy o przedłożenie listy osób upoważnionych, które będą obsługiwać ADO.	
29.	Czy osoby upoważnione do przetwarzania danych w ramach obsługi ADO zostały obowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane?	
30.	Czy podmiot przetwarzający wprowadził procedurę upoważniania osób uczestniczących w przetwarzaniu danych osobowych do ich przetwarzania?	

Oświadczam, że wszystkie informacje zawarte w niniejszej ankiecie są zgodne z prawdą.

…… ……

Data i podpisy osób upoważnionych do reprezentacji podmiotu zgodnie z KRS.

Audyt o wspomnianym zakresie odbędzie się zgodnie ze standardami opisującymi przebieg procesu testowania bezpieczeństwa systemów IT oraz obszarów systemowych podlegających weryfikacji.

Prezentacja i omówienie metodyki audytu w formie warsztatów dla 6 administratorów Zamawiającego z zakresu audytowanych technologii, połączone z prezentacją prowadzonych testów w celu nabycia odpowiednich kompetencji umożliwiających weryfikację zaleceń poaudytowych oraz wiedzy z zakresu bezpieczeństwa aplikacji, identyfikacji podatności aplikacji, technologii zwiększających bezpieczeństwo aplikacji.

Dodatkowo Wykonawca zapewni szkolenia zamknięte we Wrocławiu dla 6 osób zgodne z następującymi zagadnieniami:

CERTIFIED ETHICAL HACKER v10

WYKŁAD+WARSZTATY:

1: Wprowadzenie do etycznego hakingu (Introduction to Ethical Hacking)

2: Zbieranie informacji o ataku (Footprinting and Reconnaissance)

3: Skanowanie sieci (Scanning Networks)

4: Enumeracja (Enumeration)

5: Analiza podatności (Vulnerability Analysis)

6: Hackowanie systemu (System Hacking)

7: Złośliwe oprogramowanie (Malware Threats)

8: Monitorowanie i przechwytywanie danych (Sniffing)

9: Inżynieria społeczna – socjotechniki (Social Engineering)

10: Ataki DDoS (Denial-of-Service)

11: Przejęcie/przechwytywanie sesji (Session Hijacking)

12: Omijanie IDS, zapór Firewall i Honeypots (Evading IDS, Firewalls, and Honeypots)

13: Hakowanie serwerów sieciowych (Hacking Web Servers)

14: Hakowanie aplikacji internetowych (Hacking Web Applications)

15: Ataki przez zapytania w SQL (Injection SQL)

16: Hakowanie sieci bezprzewodowych (Hacking Wireless Networks)

17: Hakowanie mobilnych platform (Hacking Mobile Platforms)

18: Hakowanie Internetu Rzeczy (IoT Hacking)

19: Bezpieczeństwo chmury (Cloud Computing)

20: Kryptografia (Cryptography)