



Załącznik 7

**Szczegółowe wymagania dla Części 2 - Zadania 7:
Materiały dydaktyczne dla uczestników oraz
wydruk zaświadczeń dla 3334 osób
w zapytaniu ofertowym nr 4/PR3/POPC/20**

1. W ramach zadania Wykonawca jest zobowiązany do:
 - 1.1. Aktualizacji i dostosowania do wykorzystywania na tabletach iPad e-Podręcznika dla opiekunów dzieci i młodzieży
 - 1.2. Opracowania i przeprowadzenia badania ewaluacyjnego e-podręcznika wśród 3334 uczestników projektu.
 - 1.3. Przygotowania projektu i wydruku kolorowych zaświadczeń dla 3334 uczestników projektu
2. E-podręcznik powinien zostać przygotowany zarówno w formacie PDF jak również aktywnego e-podręcznika umożliwiającego uczestnikom pracę zdalną.
 - 2.1. E-Podręcznik zostanie opublikowany w sposób otwarty, przez co należy rozumieć dostępność materiałów na jednej z wolnych licencji, zapewniających możliwość dowolnego wykorzystywania utworu, tworzenia i rozpowszechniania kopii utworu w całości lub we fragmentach oraz wprowadzania zmian i rozpowszechniania utworów zależnych oraz publikację utworów przygotowanych w ramach realizowanego projektu na stronach określonych przez Zamawiającego.
 - 2.2. Wykonawca może przedstawić propozycję zmian w podręczniku w stosunku do zagadnień jakie przewidział Zamawiający.
3. Wykonawca musi przedstawić projekt ewaluacji on-line służącej, między innymi, ocenie jakości e-podręcznika i jego praktycznej przydatności. Wykonawca musi przedstawić wstępny wzór ankiety skierowanej do użytkowników w celu badania oceny e-podręcznika oraz korzyści, jakie użytkownicy odnieśli w wyniku korzystania z niego. Badanie powinno zostać przeprowadzone w oparciu o portal realizowany w ramach Zadania 6.
4. Projekt zaświadczeń dla uczestników szkoleń powinien uwzględniać wszystkie wytyczne Zamawiającego oraz uzyskać jego akceptację.
5. Zadanie 7 powinno zostać zrealizowane w terminie 90 dni od podpisania umowy.
6. Poniżej przedstawiono spis treści podręcznika posiadanego przez Zamawiającego:
 - Podstawowe środki zapewniania bezpieczeństwa
 - Internet
 - Internet w życiu młodych ludzi
 - Czy Internet jest bezpieczny?
 - Urządzenia mobilne
 - Przegląd zagrożeń sieci
 - Oprogramowanie
 - Co to jest aktualizacja oprogramowania?
 - Korzyści z aktualizacji
 - Wersja oprogramowania
 - Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10
 - Sprawdzanie dostępności aktualizacji
 - Co to jest konto użytkownika?
 - Tożsamość użytkownika
 - Rodzaje kont użytkowników
 - Uwierzytelnianie a autoryzacja
 - Alternatywne metody uwierzytelniania
 - Konta w systemie Windows 10
 - Tworzenie i usuwanie kont



Fundusze Europejskie
Polska Cyfrowa

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Zarządzanie kontami w Windows 10
Zmiana roli konta/ usunięcie konta
Praca w kontekście Użytkownika standardowego
Dobre praktyki w tworzeniu haseł
Co to jest silne hasło i jak je tworzyć?
Po co mi hasło, które wszyscy znają?
Socjotechnika w wyłudzeniu haseł
Inne sposoby zabezpieczania urządzeń
System operacyjny i aplikacje służące do jego ochrony.
Firewall – zaporę sieciową
Windows Defender
Ochrona danych w komputerze
Certyfikaty i zabezpieczanie danych
Programy do szyfrowania danych
Podstawowe informacje o wirusach i złośliwym oprogramowaniu
Jak może dojść do infekcji
Oprogramowanie antywirusowe i antyspyderskie
Co to jest kopia zapasowa?
Do czego może się przydać?
Jak chronić ważne dla nas pliki
Tworzenie kopii zapasowej
Punkt przywracania w systemie
Kopie plików i ważnych dokumentów.
Doxware
Dane niebezpieczne i nielegalne
Czym jest prawo autorskie
Plagiaty
Podsumowanie ABC bezpieczeństwa
Kogo zawiadomić w przypadku znalezienia danych niebezpiecznych lub nieodpowiednich
Złośliwe oprogramowanie
Co to jest złośliwe oprogramowanie?
Skala zjawiska
Wirusy komputerowe
Crimeware
Rodzaje programów typu crimeware
Zabezpieczanie się przed oprogramowaniem typu Crimeware
Metody rozpowszechniania się złośliwego oprogramowania (poczta, sieć internetowa, nośniki danych)
Rozprzestrzenianie się złośliwego oprogramowania
Programy zabezpieczające przed złośliwym oprogramowaniem
Skanery online
Konfiguracja skanowania (typy skanowania)
Profilaktyka antywirusowa
Potencjalne objawy infekcji wirusowej.
Legalne źródła a złośliwe oprogramowanie.
Postępowanie w wyniku infekcji komputerowej.
Ograniczenia programów zabezpieczających komputer przed złośliwym oprogramowaniem
Poczta elektroniczna
Spam i jego ograniczanie
Spam
Filtr – program antyspamowy
Jak bronić się przed spamem
Spam a prawo
Spam – praktyki handlowe
Wiadomości zawierające złośliwe oprogramowanie



Fundusze Europejskie
Polska Cyfrowa

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Jak postępować z załącznikami
Na czym polega metoda zwana Phishing
Jak się bronić przed phishingiem?
SSL/TLS
Co to jest certyfikat bezpieczeństwa?
Ochrona prywatności
Znajomość praw i obowiązków
Prawa ucznia (dziecka)
Poszanowanie godności osobistej
Nietykalność osobista
Telefony komórkowe w szkole
Ochrona danych osobowych
Monitoring w szkole a prywatność
Publikowanie zdjęć a prywatność
Niebezpieczne wywiadówki
Polityka prywatności
Co to jest GIDDO
Poczta – wiadomości
Konfigurowanie programu pocztowego
Przekierowywanie wiadomości
Filtrowanie wiadomości i blokowanie nadawców
Filtrowanie spamu
Blokowanie wiadomości
Białe i czarne listy
Komunikatory
Przykłady komunikatorów
Funkcje komunikatorów
Ochrona prywatności podczas pracy z komunikatorami
Snapchat
Dlaczego ten komunikator został wyróżniony osobnym zapisem?
Wiadomości tekstowe (SMS)
Wiadomości multimedialne (MMS)
Komunikacja Bluetooth
Wysyłanie wiadomości poczty elektronicznej
Komunikacja przez Wi-Fi
Komunikacja Irda
Postępowanie w przypadku zawartości niebezpiecznej lub nieodpowiedniej
Bezpieczne przeglądanie zasobów WWW i płatności w Internecie
Trzynastoletni użytkownik serwisu/banku a prawo
Podstawowe zasady bezpieczeństwa
Ciasteczka i wyskakujące okienka
Wady i zalety ciasteczek
Kontrola wyskakujących okienek
Bezpieczeństwo danych osobowych
Dane osobowe
Legalne i nielegalne wykorzystywanie baz danych
Jakie dane można znaleźć na własny temat
Adres IP – czy to dane osobowe?
Ochrona danych osobowych, na co zwracać uwagę?
Gdzie szukać pomocy?
Tożsamość internetowa
Jak dochodzi do kradzieży danych osobowych
Do czego można wykorzystać skradzioną tożsamość
Jak chronić swoją tożsamość



Fundusze Europejskie
Polska Cyfrowa

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Co jeśli zauważysz coś podejrzanego
Szyfrowanie komunikacji
Rozróżnianie stron szyfrowanych i nieszyfrowanych
Rodzaje kluczy szyfrowania
Długość szyfru a siła szyfrowania
Sposoby płatności przez Internet
Karty wirtualne
Przebieg transakcji – zabezpieczenia banków
Aukcje internetowe
Systemy płatności
Kontakt z administratorem serwisu, bankowego, aukcyjnego
Postępowanie w przypadku znalezienia stron niebezpiecznych lub nielegalnych
Bezpieczeństwo dzieci
Co to jest cyberprzestrzeń
Jak może pomóc Ci rodzic lub nauczyciel
Rola rodzica w przygotowaniu dziecka do kontaktu z elektronicznym światem zewnętrznym
Czym są cyberprzestępstwa
Jakie formy przyjmują cyberprzestępstwa
Niebezpieczne kontakty
Niebezpieczne treści
Cyber
Cyberprzemoc
Formy cyberprzemocy
Uzależnienie
Cyberprzestępstwa
Mailowy scam
Spam
Cyberteroryzm
Pozorna bezkarność i anonimowość
Profilaktyka
Niebezpieczne kontakty:
Niebezpieczne treści
Cyberprzemoc
Ha ha ha. Jestem świadkiem!!! :-(
Uzależnienia
Podsumowanie
Przeglądanie historii przeglądarki
Włączania i praca w trybie prywatnym
Kontrola rodzicielska
Na czym polega monitorowanie komputera
Oprogramowanie chroniące komputer
Aplikacje ułatwiające monitorowanie
Identyfikowanie procesu skojarzonego z programem
Kończenie procesu
Kontrola rodzicielska
Korzystanie z mechanizmu Safe Search
Oprogramowanie chroniące komputer
Programy antywirusowe
☐Programy anty-spamowe
FireWall
Przeglądanie i archiwizacja rozmów komunikatorów i chatów.
Jak przejrzeć archiwum rozmów komunikatora internetowego
Przeglądanie zapisu z czatu
Bezpieczne strony i wyszukiwarki dla dzieci



Wyszukiwarki i katalogi dedykowane dla dzieci i nastolatków

Wyszukiwarki stron dla dzieci

Bezpieczne strony przeznaczone dla dzieci

Sposoby komunikacji z administratorami serwera

Blokada niebezpiecznych stron

Zgłaszanie stron zawierających nielegalne treści

Oznaczenia klasyfikacji PEGI

Co to jest PEGI (Pan European Game Information)

Klasyfikacja pierwsza to tak zwane ratingi wiekowe.

Oznaczenie „PEGI OK

Aplikacje mobilne185

Ukryte koszty oraz zakupy wewnątrz aplikacji

Challeng-e / Wyzwania

7. Opis kryteriów jakimi Zamawiający będzie się kierował przy wyborze oferty.

7.1. Zamawiający dokona oceny części merytorycznej oferty na zasadzie zawiera/nie zawiera następujących elementów:

7.1.1. szczegółowy opis koncepcji wykonania e-podręcznika z opisem wszystkich funkcji uwzględniający wszystkie wymagania Zamawiającego

7.1.2. opis ewaluacji e-podręcznika

7.1.3. Oferta nie zawierająca nawet jednego z powyższych elementów będzie odrzucona.

7.2. Kryteria oceny ofert:

7.2.1. Za najkorzystniejszą zostanie uznana oferta, która nie podlega odrzuceniu oraz uzyska największą ilość punktów obliczonych wg wzoru:

$P = CE + MO + WZ$, gdzie:

P – całkowita liczba punktów;

CE – ocena punktowa za kryterium „zaoferowana cena oferty”

MO - ocena punktowa za kryterium „minimalna objętość” e-podręcznika

WZ – ocena punktowa za kryterium „podwyższenie zabezpieczenia gwarancji wykonania usługi/dostawy”

Punkty będą obliczane z dokładnością do 2 miejsc po przecinku. Dla pozostałych pozycji będą stosowane zaokrąglenia. Oferta może uzyskać max 100 punktów.

7.2.2. Ocena punktowa za kryterium „zaoferowana cena oferty”

Za część „zaoferowana cena oferty” (CE) oferta może uzyskać max 40 pkt.

Obliczanie punktów dla tej części będzie się odbywać wg wzoru:

$CE = (C_{min}/C) * 40$

Gdzie:

CE-ocena punktowa za kryterium „zaoferowana cena oferty”

C_{min}-najniższa cena brutto całości zamówienia zaoferowana w postępowaniu

C-cena brutto całości zamówienia zaoferowana przez Wykonawcę w ofercie, np:

I oferta – cena 400,00 PLN to $(100/400) * 40 = 10,00$ pkt.

II oferta – cena 200,00 PLN to $(100/200) * 40 = 20,00$ pkt.

III oferta – cena 100,00 PLN to $(100/100) * 40 = 40,00$ pkt.

7.2.3. Ocena punktowa za kryterium „minimalna objętość” e-podręcznika



Fundusze Europejskie
Polska Cyfrowa

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Za deklarowaną minimalną liczbę znaków w finalnym e-podręczniku (MO) oferta może uzyskać max 20 pkt.

Obliczanie punktów dla tej części będzie się odbywać wg wzoru:

$$MO = (O / O_{max})$$

Gdzie:

MO- Ocena punktowa za kryterium „minimalna objętość” e-podręcznika

O_{max} - największa deklarowana objętość finalnego e-podręcznika liczona w znakach zaoferowana w postępowaniu

O- deklarowana minimalna objętość finalnego e-podręcznika wyrażona w znakach zaoferowana przez Wykonawcę w ofercie, np:

I oferta – 10 000 znaków to $(10\,000 / 50\,000) * 20 = 4,00$ pkt.

II oferta – 20 000 znaków to $(20\,000 / 50\,000) * 20 = 8,00$ pkt.

III oferta – 50 000 znaków to $(50\,000 / 50\,000) * 20 = 20,00$ pkt.

7.2.4. Ocena punktowa za kryterium „podwyższenie zabezpieczenia gwarancji wykonania usługi/dostawy”

Oferta może dodatkowo otrzymać max 40 punktów za podwyższenie gwarancji zabezpieczenia wykonania usługi/dostawy (Wz):

$$Wz = (G / G_{max}) * 40$$

gdzie:

Wz-wynik

G_{max}-najwyższa wartość procentowa gwarancji ponad wartość wymaganą zaoferowana w postępowaniu zamieniona na ułamek dziesiętny

G-wartość procentowa gwarancji zaoferowana ponad wartość wymaganą w ocenianej ofercie zamieniona na ułamek dziesiętny

W przypadku gdy Oferent zaoferuje zabezpieczenie na minimalnym wymaganym poziomie wówczas oferta dla kryterium Wz uzyska 0 pkt. np.

I oferta – zabezpieczenie wynosi 20% (min. wartość wymagana) to Wz=0 pkt.

II oferta - zabezpieczenie wynosi 25% to $(0,5/1) * 40 = 20$ pkt.

III oferta - zabezpieczenie wynosi 30% to $(1/1) * 40 = 40$ pkt.