POWIAT TATRZAŃSKI

✉ **ul. Chramcówki 15, 34-500 Zakopane**

☎ tel. (+48 18) 20-17-100 🖳 http://www.powiat.tatry.pl
☎ fax (+48 18) 20-17-104 🖳 e-mail: zp@powiat.tatry.pl

Zakopane, dnia 30 stycznia 2018 roku

ZP.270.1.2018
pyt. i odp. do Zaproszenia – Nr 2

Wykonawcy Pobierający
Materiały Przetargowe
Zaproszenie do złożenia oferty
Wszyscy

W wyniku otrzymanych pisemnych pytań dotyczących postępowania na: **„Wykonanie usługi w zakresie przygotowania dokumentacji wg norm w zakresie bezpieczeństwa informacji oraz jej wdrożenie dla Starostwa Powiatowego w Zakopanem”** działając na podstawie punktu VI.8 zaproszenia do złożenia oferty, przesyłam Państwu treść pisemnych pytań, odpowiedzi związaną z udzielonymi wyjaśnieniami na zadane pytania oraz treść modyfikacji, zmian zapisów przedmiotowego Zaproszenia.

I. Pytania i odpowiedzi do Zaproszenia:

Przesyłam Państwu treść pisemnych pytań oraz wyjaśnienia na zadane pytania w związku z przedmiotowym postępowaniem:

1. **Pytanie 1**
   W specyfikacji zaproszenia do składania ofert dla zadania Bezpieczeństwo Informacji - ZP.270.1.2018, w załączniku nr 5 do zaproszenia "Opis przedmiotu zamówienia", w rozdziale III "Wymagania dotyczące realizacji przedmiotu zamówienia", podrozdział "Zakres realizacji przedmiotu zamówienia", "Etap 1", pkt 1.2 zostało zawarte wymaganie:
   "Wykonawca przekaże Zamawiającemu 1 egzemplarz norm w języku polskim w wersji elektronicznej dla Zamawiającego z prawami ich użytkowania:
   1.2.1. PN-ISO/IEC 27001,
   1.2.2. PN-ISO/IEC 27002,
   1.2.3. PN-ISO/IEC 27005,
   1.2.4. PN-ISO/IEC 22301,
   1.2.5. PN-ISO/IEC 24762."
   Zgodnie z ustawa o normalizacji i wynikającymi z niej warunkami udzielania licencji ze strony przez Polski Komitet Normalizacji, PKN udziela licencji na zakup i prawa ich użytkowania podmiotowi dokonującymi płatność bez prawa do przenoszenia własności. Podmiot płacący za zakup norm nie może również wskazać podmiotu na rzecz którego mają być wystawione licencje i normy.

Co za tym idzie jeżeli wykonawca zapłaci za w/w normy, to licencja zostanie przypisana do Wykonawcy bez prawa jej przepisani na Zamawiającego.
Czy w związku z powyższym wymaganie zostanie utrzymane?

Odpowiedź: Zamawiający informuje i wyjaśnia, że postanawia dokonać zmiany, modyfikacji zapisów Zaproszenia, w zakresie załącznika nr 5 do Zaproszenia "Opis przedmiotu zamówienia", rozdzial III "Wymagania dotyczące realizacji przedmiotu zamówienia", podrozdział "Zakres realizacji przedmiotu wdrożenia", dotyczący "Etap 1", w którym punkt 1.2 **podlega wykreśleniu**.

W związku z powyższym ulega zmianie, modyfikacji opis przedmiotu zamówienia (załącznik nr 5 do Zaproszenia), patrz część II niniejszego pisma – Modyfikacja zmiana zapisów Zaproszenia.

_____

II.

2. Pytanie 1

Na stronie 5 SIWZ Zamawiający opisał warunek udziału w postępowaniu Wykonawca zobowiązany jest wykazać, że dysponuje osobą posiadającą certyfikat CISSP lub ITIL lub inny równoważny w zakresie bezpieczeństwa systemów informatycznych wydanym przez jednostkę certyfikującą wskazanego w wykazie, o którym mowa powyżej w punkcie 3b) specjalisty ds. bezpieczeństwa systemów informatycznych. Czy Zamawiający uzna za równoważny certyfikat CEH lub OSCP?
Wykonawca posiada pracowników, posiadających certyfikaty Certified Ethical Hacker oraz Offenssive Security Certified Professional. Certyfikat CEH https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ potwierdza, że osoba go posiadająca ma odpowiednią wiedzę i umiejętności, co agresor próbujący przełamać bariery bezpieczeństwa. Z kolei certyfikat OSCP https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/ potwierdza praktyczne umiejętności w zakresie prowadzenia audytów oraz testów bezpieczeństwa. Osoby posiadające ten certyfikat, muszą poprzez wskazanie wad symulowanych środowisk informatycznych, udowodnić swoje kompetencje w wymiarze praktycznym.

Odpowiedź: Zamawiający informuje i wyjaśnia, że postanawia dokonać zmiany, modyfikacji zapisów Zaproszenia, w zakresie punktu IV.5) oraz punktu VIII.2 Zaproszenia, która ma na celu uwzględnienie złożonego wniosku.

W związku z powyższym ulega zmianie, modyfikacji punktu IV.5.5) oraz punktu VIII.2 Zaproszenia oraz wzór wykazu osób, skierowanych przez wykonawcę do realizacji zamówienia (załącznik nr 3 do Zaproszenia), patrz część II niniejszego pisma – Modyfikacja zmiana zapisów Zaproszenia.

II. Modyfikacja (zmiana) zapisów Zaproszenia:

Postanawia się wprowadzić modyfikacje, zmiany zapisów przedmiotowego Zaproszenia, które stają się jego integralną częścią. Dokonane zmiany są wiążące dla Wykonawców, którzy pobrali materiały przetargowe (Zaproszenie).

1. **<u>Ulega zmianie punkt IV.5) Zaproszenia, który otrzymuje nowe brzmienie:</u>**

„ Punkt IV.5.5) Ewentualnie (w przypadku posiadania) certyfikat CISSP lub ITIL lub CEH lub OSCP lub inny równoważny w zakresie bezpieczeństwa systemów informatycznych wydanym przez jednostkę certyfikującą wskazanego w wykazie, o którym mowa powyżej w punkcie 3b) specjalisty ds. bezpieczeństwa systemów informatycznych.

2. **<u>Ulega zmianie punkt VIII.2 Zaproszenia, który otrzymuje nowe brzmienie:</u>**

„ Punkt VIII.2 Powyższym kryteriom zamawiający przypisał następujące znaczenie:

Kryterium	Waga [%]	Liczba punktów	Sposób oceny
Łączna cena ofertowa brutto	**85%**	**85**	Cena najtańszej oferty C = ---------- x 85 pkt Cena badanej oferty
Jakość	**15%**	**15**	1. Audytor systemów zarządzania bezpieczeństwem informacji legitymujący się udziałem, w przeciągu ostatnich pięciu lat przed upływem terminu składania ofert, w realizacji projektów w roli audytora lub konsultanta w zakresie wdrożenia systemu zarządzania bezpieczeństwem informacji o wartości minimum 20.000,00 PLN brutto: • w co najmniej 2 projektach – 0 punktów, • w 3 - 4 projektach – 3 punkty, • w 5 i więcej projektach – 5 punktów. 2. Specjalista ds. bezpieczeństwa systemów informatycznych: • posiadający certyfikatem CISSP lub ITIL lub CEH lub OSCP lub inny równoważny w zakresie bezpieczeństwa systemów informatycznych wydanym przez jednostkę certyfikującą – 10 punktów, • brak certyfikatu – 0 punktów.
RAZEM	**100%**	**100**	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

3. **<u>Ulega zmianie załącznik nr 3 do Zaproszenia – Wzór wykazu osób, skierowanych przez wykonawcę do realizacji zamówienia, który otrzymuje nowe brzmienie:</u>**

Nowy zmodyfikowany wyjaśnieniami z dnia 30 stycznia 2018 roku wzór wykazu osób, skierowanych przez wykonawcę do realizacji zamówienia będący załącznikiem nr 3 do Zaproszenia, jest dołączony do niniejszego pisma w postaci załącznika nr 1.

4. **<u>Ulega zmianie załącznik nr 5 do Zaproszenia – Opis Przedmiotu Zamówienia, który otrzymuje nowe brzmienie:</u>**

Nowy zmodyfikowany wyjaśnieniami z dnia 30 stycznia 2018 roku Opis Przedmiotu Zamówienia będący załącznikiem nr 5 do Zaproszenia, jest dołączony do niniejszego pisma w postaci załącznika nr 2.

W wyniku dokonania powyższych wyjaśnień, a zarazem modyfikacji, zmian zapisów przedmiotowego Zaproszenia do udziału w postępowaniu zamawiający postanawia dokonać zmiany terminu do składania ofert, a to:

5. <u>Ulega zmianie punkt IV.3 Zaproszenia, który otrzymuje nowe brzmienie:</u>

„ Punkt IV.3 Ofertę należy złożyć w zamkniętej nieprzeźroczystej kopercie lub opakowaniu, w siedzibie zamawiającego i oznakować w następujący sposób:

Nazwa i adres wykonawcy:
……
……

Starostwo Powiatowe w Zakopanem
ul. Chramcówki 15, 34-500 Zakopane
Dziennik Podawczy

OFERTA PRZETARGOWA
Wykonanie usługi w zakresie przygotowania dokumentacji wg norm w zakresie bezpieczeństwa informacji oraz jej wdrożenie dla Starostwa Powiatowego w Zakopanem – znak: ZP.270.1.2018
Nie otwierać przed: 05 lutego 2018 roku przed godz. 11:15

6. <u>Ulega zmianie punkt VII.2 Zaproszenia, który otrzymuje nowe brzmienie:</u>

„ Punkt VII.2 Ofertę należy złożyć w terminie: **<u>do dnia 05 lutego 2018 roku, do godziny 11:00</u>**.

7. <u>Ulega zmianie punkt VII.3 Zaproszenia, który otrzymuje nowe brzmienie:</u>

„ Punkt VII.3 Otwarcie ofert nastąpi **w dniu 05 lutego 2018 roku o godzinie 11:15**.

Załączniki:
1. Załącznik nr 1 – Zmodyfikowany wzór wykazu osób, skierowanych przez wykonawcę do realizacji zamówienia (załącznik nr 3 do Zaproszenia),
2. Załącznik nr 2 – Zmodyfikowany Opis Przedmiotu Zamówienia (załącznik nr 5 do Zaproszenia),

UWAGA !!!
Powyższe zmiany należy uwzględnić w składanej ofercie przetargowej.

Z poważaniem:

STAROSTA TATRZAŃSKI

mgr inż. Piotr Bąk

Otrzymują:
1. Wykonawcy, którzy pobrali Zaproszenie,
2. A/a.

Załącznik nr 3 do zaproszenia

WYKAZ
OSÓB, SKIEROWANYCH PRZEZ WYKONAWCĘ DO REALIZACJI ZAMÓWIENIA

Przystępując do postępowania pn.: **Wykonanie usługi w zakresie przygotowania dokumentacji wg norm w zakresie bezpieczeństwa informacji oraz jej wdrożenie dla Starostwa Powiatowego w Zakopanem**

Działając w imieniu Wykonawcy: ……
……
……
……
(podać nazwę i adres Wykonawcy)

Składam wykaz osób, skierowanych do realizacji zamówienia, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami.

1.	Imię i Nazwisko	
	Kwalifikacje zawodowe / Uprawnienia	Audytor systemów zarządzania bezpieczeństwem informacji legitymujący się udziałem, w przeciągu ostatnich pięciu lat przed upływem terminu do składania ofert, w przynajmniej dwóch projektach w roli audytora lub konsultanta w zakresie wdrożenia systemu zarządzania bezpieczeństwem informacji. Wartość zamówienia każdego wskazanego projektu nie może być mniejsza niż 20.000,00 PLN brutto (słownie złotych: dwadzieścia tysięcy). Audytor systemów zarządzania bezpieczeństwem informacji posiada znajomość normy ISO/IEC 27001 potwierdzonej certyfikatem (Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001) wydanym przez jednostkę certyfikującą. **TAK* / NIE*** **UWAGA** **Do składanej oferty należy dołączyć stosowny certyfikat**
	Doświadczenie i wykształcenie niezbędnych do wykonania zamówienia	
	Ilość udziałów w przeciągu ostatnich pięciu lat przed upływem terminu do składania ofert w projektach w roli audytora lub konsultanta w zakresie wdrożenia systemu zarządzania bezpieczeństwem informacji, których wartość wynosiła minimum 20.000,00 PLN brutto	
	Zakres wykonywanych czynności	Audytor systemów zarządzania bezpieczeństwem informacji
	Oświadczam, że dysponuje* / będę dysponował* w/w osobą * niepotrzebne skreślić	
2.	Imię i Nazwisko	
	Kwalifikacje zawodowe / Uprawnienia	Specjalista ds. bezpieczeństwa systemów informatycznych posiadający wiedzę i doświadczenie w zakresie bezpieczeństwa systemów informatycznych, poparte udziałem w minimum dwóch zrealizowanych projektach, przy czym wartość co najmniej jednego projektu wynosiła minimum 20.000,00 PLN brutto (słownie złotych: dwadzieścia tysięcy). **TAK* / NIE***

	Doświadczenie i wykształcenie niezbędnych do wykonania zamówienia	
	Specjalista posiada certyfikat CISSP lub ITIL lub CEH lub OSCP lub innym równoważny w zakresie bezpieczeństwa systemów informatycznych wydanym przez jednostkę certyfikującą	**TAK* / NIE*** **UWAGA** **W przypadku skazania opcji TAK do składanej oferty należy dołączyć stosowny certyfikat**
	Zakres wykonywanych czynności	Specjalista ds. bezpieczeństwa systemów informatycznych
	Oświadczam, że dysponuje* / będę dysponował* w/w osobą * niepotrzebne skreślić	

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI

Oświadczam, że wszystkie informacje podane w niniejszym oświadczeniu są zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

.....	.....
Pieczęć Wykonawcy	Data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik nr 5 do zaproszenia

Załącznik nr 1
do Umowy Nr ZP.270.1.2018 z dnia ……. 2018 roku

OPIS PRZEDMIOTU ZAMÓWIENIA

Szczegółowy opis przedmiotu zamówienia na wykonanie usługi w zakresie przygotowania dokumentacji wg norm w zakresie bezpieczeństwa informacji oraz jej wdrożenie w ramach projektu „E-Usługi w informacji przestrzennej w Powiecie Tatrzańskim”

I. Określenie przedmiotu zamówienia

Przedmiotem zamówienia jest **wykonanie usługi w zakresie przygotowania dokumentacji wg norm w zakresie bezpieczeństwa informacji oraz jej wdrożenie dla Starostwa Powiatowego w Zakopanem**, zgodnie z wymaganiami Krajowych Ram Interoperacyjności, normy PN-ISO/IEC 27001 oraz zaleceniami norm: PN-ISO/IEC 27005, PN-ISO/IEC 24762 jak również Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
Poprzez opracowanie dokumentacji systemu należy rozumieć: przygotowanie przez Wykonawcę dokumentów od strony merytorycznej i formalnej do stanu, który pozwala przekazać dokumenty do jednostki certyfikującej przez Zamawiającego, bez podejmowania działań redakcyjnych lub innych ingerencji w treść dokumentu ze strony Zamawiającego. Po stronie Zamawiającego leży jedynie uzgodnienie treści dokumentów z Wykonawcą. Wykonawca gwarantuje że dokumentacja:

- systemu zarządzania bezpieczeństwem informacji jest zgodna z wymaganiami Rozporządzenia 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 (Dz. U. z 2012 r., poz. 526).
- systemu zarządzania bezpieczeństwem informacji jest zgodna z wymaganiami normy ISO/IEC 27001 oraz wymaganiami certyfikacyjnymi jednostki certyfikującej systemy zarządzania na zgodność z normą ISO/IEC 27001, akredytowanej przez dowolną jednostką akredytującą wymienioną na stronie http://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4.
- bezpieczeństwa danych osobowych jest zgodna z wymaganiami Ustawy z dnia 29 sierpnia 1997 r. o Ochronie Danych Osobowych Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z

przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Zamawiający oczekuje również, że Wykonawca zrealizuje usługę polegającą na:

- zaimplementowaniu wybranych dobrych praktyk ITIL (Information Technology Infrastructure Library) lub normy PN-ISO/IEC 20000 w środowisku IT urzędu w szczególności w zakresie budowy katalogu świadczonych usług informatycznych oraz przydzieloną odpowiedzialnością pracowników za usługę (model RACI)
- przeprowadzeniu audytu bezpieczeństwa systemów teleinformatycznych

Cel projektu:

Celem projektu jest podniesienie poziomu bezpieczeństwa systemów informatycznych Starostwa Powiatowego w Zakopanem a w szczególności zapewnienie przetwarzanych informacji w Zintegrowanym Geodezyjnym Systemie Informacji oraz udostępnionym e-usługom wdrażanym w ramach projektu „E-Usługi w informacji przestrzennej w Powiecie Tatrzańskim" poprzez opracowanie dokumentacji Polityki Bezpieczeństwa Informacji, wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz zaimplementowanie dobrych praktyk w zarządzaniu i eksploatacją w środowisku IT urzędu.

Dzięki realizacji projektu PBI, spodziewane jest osiągnięcie poniższych korzyści:

- zapewnienie bezpieczeństwa danych i systemów użytkowanych przez Starostwo Powiatowe w Zakopanem a w szczególności Zintegrowanemu Geodezyjnemu Systemowi Informacji w oparciu o normy i standardy europejskie takie jak np. PN-ISO/IEC 27001,
- ograniczenie czasu niedostępności systemów informatycznych urzędu z powodów ich awarii, poprzez opracowanie Planów Ciągłości Działania,
- optymalizacja kosztów zabezpieczenia infrastruktury teleinformatycznej urzędu przed działaniem szkodliwego oprogramowania, prób włamań i zabezpieczenie procesu udostępniania danych w tym danych geodezyjnych poprzez e-usługi,
- standaryzacja rozwiązań (technologii) oraz metod budowy interfejsów,
- optymalizacja kosztów utrzymania i rozwoju systemów informatycznych.

Terminy realizacji zamówienia:

Zakończenie realizacji całości zamówienia **w terminie do 9 miesięcy od dnia podpisania umowy.** Realizacja prac objętych etapami od 1 do 3 włącznie nastąpi nie później niż do 30 kwietnia 2018 roku.

Przeznaczenie realizowanego przedmiotu Zamówienia:

Niniejszy przedmiot zamówienia stanowi jedno z działań w projekcie pn.: „E-Usługi w informacji przestrzennej w Powiecie Tatrzańskim", realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Małopolskiego na lata 2014-2020, 2 Oś priorytetowa Cyfrowa Małopolska, Działanie 2.1 E-administracja i cyfrowe zasoby, Poddziałanie 2.1.4 e-Usługi w informacji przestrzennej, mający na celu zapewnienie odpowiedniego poziomu bezpieczeństwa posiadanych informacji oraz ciągłości działania dla krytycznych urządzeń i usług w ujęciu wdrażanych rozwiązań teleinformatycznych w projekcie, w tym niezbędne jest

zapewnienie bezpieczeństwa informacji w urzędzie według obowiązujących w tym zakresie norm oraz przepisów prawa.

Oznaczenie przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

Kod i nazwa CPV:
79417000-0 – Usługi doradcze w zakresie bezpieczeństwa

II. Informacje ogólne o środowisku Zamawiającego

Przetwarzanie informacji odbywa się w jednej lokalizacji (Zakopane ul. Chramcówki 15). Zamawiający zatrudnia około 120 osób. Środowisko teleinformatyczne zawiera około 110 zestawów komputerowych, około 20 elementów aktywnych sieci informatycznej oraz około 30 serwerów fizycznych i wirtualnych. Urząd posiada serwerownię główną, zapasową oraz pomieszczenie dystrybucji.
Powiat Tatrzański jako Administrator Danych Osobowych przetwarza dane osobowe w ponad 40 zbiorach danych osobowych. Zamawiający udostępni wykonawcy do wglądu wszystkie dokumenty w tym obecnie obowiązującą Politykę Bezpieczeństwa Informacji, Instrukcję Zarządzania Systemem Informatycznym oraz zarządzenia obejmujące z zakresu bezpieczeństwa informacji, niezbędne do realizacji prac.
Szczegółowa informacje o środowisku teleinformatycznym zostaną udostępnione Wykonawcy po podpisaniu umowy.

III. Wymagania dotyczące realizacji przedmiotu zamówienia:

Projekt wdrożeniowy

W ramach realizacji zamówienia Wykonawca opracuje projekt wdrożeniowy przedmiotu zamówienia wraz z ogólnym harmonogramem realizacji prac. Projekt wdrożenia wraz z ogólnym harmonogramem prac musi być dostarczony Zamawiającemu do akceptacji przed przystąpieniem do realizacji usługi, **nie później niż 14 dni od dnia podpisania umowy.**
Dostarczony projekt musi zawierać przynajmniej:

- Ogólny harmonogram prac każdego etapu,
- Listę zadań do wykonania przez Wykonawcę i Zamawiającego.

Zamawiający ma prawo do wnoszenia uwag do przedstawionego projektu wdrożeniowego w terminie 7 dni od daty otrzymania projektu wdrożeniowego. Wykonawca zobowiązany jest do ich uwzględnienia w terminie 7 dni od daty wniesienia uwag.
Projekt wdrożeniowy będzie podlegał akceptacji przez Zamawiającego.

Dodatkowe wymagania

- Prace wdrożeniowe muszą być prowadzone w sposób niekolidujący z pracą urzędu, mając na uwadze szeroko rozumiany komfort petentów oraz pracowników.
- Formą akceptacji wszystkich prac będzie protokół odbioru, który będzie podpisywany pomiędzy Kierownikiem Projektu ze strony Wykonawcy i upoważnionym przedstawicielem Zamawiającego.

- **Wykonawca zgłosi pisemnie Zamawiającemu gotowość do odbioru wyników prac, objętych poszczególnym etapem wdrożenia przedmiotu zamówienia.**
- **Zamawiający rozpocznie weryfikację przekazanego przedmiotu zamówienia w terminie 7 dni roboczych od daty zgłoszenia gotowości odbioru.**
- W przypadku stwierdzenia przez Zamawiającego zastrzeżeń, wad, uwag bądź rozbieżności pomiędzy przekazanymi do weryfikacji wynikami danego etapu, a założeniami przyjętymi dla wykonania przedmiotu Umowy, Zamawiający sporządzi i przekaże Wykonawcy protokół rozbieżności.
- Po otrzymaniu protokołu rozbieżności, Wykonawca w terminie 7 dni roboczych lub innym wzajemnie uzgodnionym terminie dokona koniecznych poprawek, zmian lub udzieli wiążących wyjaśnień w tej sprawie i przekaże wyniki danego etapu do ponownej weryfikacji.
- Odbiór wykonanych prac uważa się za zakończony z chwilą podpisania bez zastrzeżeń odpowiedniego protokołu odbioru przez obie Strony, w ilości po jednym egzemplarzu dla każdej ze Stron

Wykonawca ma zapewnić pracowników do realizacji projektu posiadających niezbędną wiedzę do należytego wykonania przedmiotu umowy

Zakres realizacji przedmiotu wdrożenia:

Etap 1 – Audyt zerowy

1. Wykonawca przeprowadzi spotkanie wprowadzające dla kadry zarządzającej, kierowników komórek organizacyjnych oraz pracowników w zakresie celów i zasad funkcjonowania SZBI, ochrony informacji, inwentaryzacji i klasyfikacji aktywów chronionych oraz szacowania ryzyka. W spotkaniu będzie uczestniczyć ok. 20 osób (maksymalnie w 2 grupach).
   1.1. Zakres potkania obejmować:
      1.1.1. Przedstawienie celów projektu, harmonogramu oraz oczekiwanych rezultatów na poszczególnych etapach,
      1.1.2. Omówienie wymagań normy PN-ISO/IEC 27001,
      1.1.3. Wprowadzenie do zarządzania ryzykiem,
      1.1.4. Omówienie roli i obowiązków zespołu roboczego PBI w projekcie,
      1.1.5. Sposób komunikacji na dalszych etapach projektu między Wykonawcą a Zamawiającym,
   1.2. Wykonawca zobowiązany jest ponadto do przygotowania i przedłożenia Zamawiającemu imiennej listy obecności uczestników spotkania,
2. Zakres prac audytu wstępnego będzie obejmował co najmniej:
   2.1. Zapoznanie się ze strukturą organizacyjną Starostwa Powiatowego w Zakopanem,
   2.2. Analizę i ocenę dokumentacji w zakresie bezpieczeństwa informacji, w tym regulaminów, procedur bezpieczeństwa, zarządzeń, instrukcji oraz innych dokumentów, które Zamawiający udostępni Wykonawcy do analizy. Zamawiający zastrzega sobie prawo do udostępnienia dokumentacji tylko i wyłącznie w jego siedzibie.
   2.3. Wywiady analityczne z wytypowanymi przez Zamawiającego pracownikami poszczególnych komórek organizacyjnych w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa narzucanych normą PN ISO/ IEC 27001 oraz wewnętrznymi uregulowaniami urzędu.

3. Audyt zostanie przeprowadzony w siedzibie Starostwa Powiatowego w Zakopanem, Zakopane ul. Chramcówki 15.
4. Produktami zadania będą co najmniej:
   4.1. Materiały szkoleniowe – wprowadzenie do problematyki ochrony informacji
   4.2. Raport z audytu wstępnego.

Etap 2 – Audyt zasadniczy

1. Audyt zostanie przeprowadzony we wszystkich komórkach organizacyjnych Starostwa Powiatowego w Zakopanem z wyłączeniem informacji niejawnych.
2. Audyt zasadniczy będzie obejmował:
   2.1. **Wykonanie harmonogramu audytu**
      2.1.1. Wykonawca przed rozpoczęciem prac zobowiązany jest przedstawić Zamawiającemu do akceptacji szczegółowy harmonogram audytu,
      2.1.2. Produkty zadania: Szczegółowy harmonogram audytu
   2.2. **Przegląd kluczowych zbiorów danych**
      2.2.1. Wykonawca dokona przeglądu kluczowych zbiorów informacji przetwarzanych przez Zamawiającego w postaci elektronicznej i papierowej pod kątem ich znaczenia dla osiągania celów organizacji i zgodności z normami oraz zaproponuje przypisanie właścicieli kluczowych zbiorów informacji. Wykonawca dokona również analizę procedur bezpieczeństwa, które winny być opisane dla zidentyfikowanych zbiorów informacji. Zamawiający udostępni na tym etapie wszystkie dostępne materiały, analizy i audyty, które do tej pory były już wykonane.
      2.2.2. Produkty zadania:
         2.2.2.1. Spis kluczowych zbiorów informacji przetwarzanych przez Zamawiającego wraz z oceną ich znaczenia dla osiągania celów organizacji i zgodności z normami oraz spisem właścicieli zidentyfikowanych zbiorów informacji.
         2.2.2.2. Spis procedur bezpieczeństwa dla zidentyfikowanych zbiorów informacji.
   2.3. **Klasyfikacja zbiorów danych**
      2.3.1. W ramach procesu klasyfikacji zidentyfikowanych aktywów Wykonawca jest zobowiązany do zrealizowania następujących prac:
         2.3.1.1. Opracowanie metody klasyfikowania informacji przetwarzanych w Starostwie Powiatowym w Zakopanem,
         2.3.1.2. Opracowanie modelu podziału informacji przetwarzanych w Starostwie Powiatowym w Zakopanem w zależności od poziomu ich wrażliwości i przeznaczenia z wyłączeniem informacji niejawnych,
         2.3.1.3. Sklasyfikowanie wspólnie z pracownikami poszczególnych komórek organizacyjnych informacji przetwarzanych w Starostwie Powiatowym w Zakopanem,
         2.3.1.4. Opracowanie raportu z procesu klasyfikacji informacji na podstawie danych uzyskanych w trakcie realizacji w/w procesu,
         2.3.1.5. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej przez Wykonawcę metodyki klasyfikowania informacji, nie później jednak niż na 7 dni roboczych przed rozpoczęciem szkoleń pracowników

Starostwa Powiatowego w Zakopanem w zakresie sposobu klasyfikowania informacji,

2.3.1.6. Uwagi, o których mowa w pkt. 2.3.1.4. muszą zostać uwzględnione przez Wykonawcę,

2.3.1.7. Dokumentację, o której mowa w pkt. 2.3.1.1., a w szczególności opis metodyki klasyfikowania informacji oraz raport z procesu klasyfikowania informacji Wykonawca przekaże Zamawiającemu w formie cyfrowego repozytorium dokumentów. Forma elektroniczna dokumentacji będzie przygotowana w plikach edytowalnych.

2.3.2. Produkty zadania:

2.3.2.1. Metoda klasyfikacji informacji

2.3.2.2. Model podziału informacji przetwarzanych w Starostwie Powiatowym w Zakopanem w zależności od poziomu ich wrażliwości i przeznaczenia.

2.3.2.3. Materiały szkoleniowe dotyczące sposobu klasyfikacji informacji

2.3.2.4. Raport z procesu klasyfikacji informacji

2.4. **Przegląd i klasyfikacja aktywów przetwarzających dane**

2.4.1. Wykonawca dokona rozpoznania i klasyfikacji aktywów przetwarzających kluczowe zbiory informacji wykorzystywanych przez Zamawiającego dla informacji w postaci elektronicznej jak i tradycyjnej – papierowej oraz przypisze do nich właścicieli. Wykonawca wykona również analizę procedur bezpieczeństwa, które winny być opisane dla zidentyfikowanych aktywów.

2.5. **Weryfikacja zabezpieczeń organizacyjnych i technicznych**

2.5.1. Wykonawca przeprowadzi weryfikację stosowanych zabezpieczeń organizacyjnych i technicznych na zgodność z wymaganiami normy ISO/IEC 27001, w szczególności:

2.5.1.1. Wykonawca przeprowadzi analizę efektywności zabezpieczeń organizacyjnych wykorzystywanych przez Zamawiającego obejmującą:

2.5.1.1.1. Regulamin bezpieczeństwa (A.5)

2.5.1.1.2. Organizacja bezpieczeństwa informacji (A.6)

2.5.1.1.3. Zarządzanie aktywami (A.7)

2.5.1.1.4. Bezpieczeństwo zasobów ludzkich (A.8)

2.5.1.1.5. Bezpieczeństwo fizyczne i środowiskowe (A.9)

2.5.1.1.6. Zarządzanie systemami i sieciami (A.10)

2.5.1.1.7. Kontrola dostępu (A.11)

2.5.1.1.8. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych (A.12)

2.5.1.1.9. Zarządzanie incydentami związanymi z bezpieczeństwem informacji (A.13)

2.5.1.1.10. Zarządzanie ciągłością działania (A.14)

2.5.1.1.11. Zgodność (A.15)

2.5.1.2. Obserwacje budynków, pomieszczeń, działań i zachowań pracowników,

2.5.1.3. Analizę bezpieczeństwa systemów teleinformatycznych użytkowanych przez Zamawiającego.

2.6. **Zgodność podstaw prawnych**

2.6.1. Wykonawca zbada zgodność działań Zamawiającego ze wszystkimi wskazanymi przez Zamawiającego uregulowaniami prawnymi, którym podlega Starostwo

Powiatowe w Zakopanem w zakresie bezpieczeństwa informacji, a w szczególności z:

2.6.1.1. Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,

2.6.1.2. Rozporządzeniem MSWiA z dnia 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,

2.6.1.3. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

2.6.1.4. Rozporządzeniem 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,

2.6.1.5. z innymi ustawami i rozporządzenia, którym podlega Zamawiający.

2.7. **Dokument raportu z audytu**

2.7.1. Wykonawca jest zobowiązany do opracowania kompletnego raportu z przeprowadzonego audytu. Raport z audytu będzie zawierał w szczególności:

2.7.1.1. Cel i zakres audytu,

2.7.1.2. Szczegółowy opis przeprowadzonych prac,

2.7.1.3. Szczegółowy opis poziomu spełnienia każdego z wymagań normy PN-ISO/IEC 27001 opisanych w załączniku A do niniejszej normy,

2.7.1.4. Wykaz stwierdzonych niezgodności w odniesieniu do każdego z wymagań normy PNISO/IEC 27001 zgodnie z załącznikiem A na poziomie opisu poszczególnych zabezpieczeń wraz z przedstawieniem dowodów na istnienie niezgodności,

2.7.1.5. Rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności w odniesieniu do każdego z wymagań normy PN ISO/IEC 27001 opisanego w załączniku A,

2.7.1.6. Podsumowanie i wnioski,

2.7.2. Wykonawca opracuje osobny audyt albo uwzględni w raporcie z audytu o którym mowa w pkt. 2.7.1., raport KRI z przeprowadzonego audytu dotyczącego spełnienia wymagań paragrafu 20 ust. 1 i 2 rozporządzenia 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 (Dz. U. z 2012 r., poz. 526) przeprowadzonego przez audytora bezpieczeństwa informacji klasyfikowanego zgodnie z normą PN-EN ISO 19011 dla normy ISO/IEC 27001

2.7.3. Raport Wykonawca przekaże Zamawiającemu w formie elektronicznej w postaci dokumentacji na CD/DVD oraz papierowej. Forma elektroniczna raportów będzie przygotowana w plikach edytowalnych.

2.7.4. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu,

2.7.5. Wykonawca zobowiązany jest do uwzględnienia w raporcie wniesionych przez Zamawiającego uwag do raportu,

2.7.6. Produkty zadania:
- 2.7.6.1. Wykaz aktywów wykorzystywanych przy przetwarzaniu kluczowych zbiorów informacji wraz z ich właścicielami,
- 2.7.6.2. Klasyfikacja aktywów przetwarzających informacje w Starostwie Powiatowym w Zakopanem,
- 2.7.6.3. Spis procedur bezpieczeństwa dla zidentyfikowanych aktywów przetwarzających informacje w Starostwie Powiatowym w Zakopanem,
- 2.7.6.4. Raport z analizy efektywności zabezpieczeń organizacyjnych wykorzystywanych przez Zamawiającego,
- 2.7.6.5. Raport z analizy zgodności działań Zamawiającego ze wszystkimi wskazanymi przez Zamawiającego, uregulowaniami prawnymi, którym podlega Starostwo Powiatowe w Zakopanem w zakresie bezpieczeństwa informacji
- 2.7.6.6. Robocza wersja raportu z przeprowadzonego audytu do akceptacji Zamawiającego.

Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Starostwie Powiatowym w Zakopanym

1. W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Starostwie Powiatowym w Zakopanem, a w szczególności:
   - 1.1. Opracować metodykę szacowania ryzyka spełniającą wymagania PN-ISO/IEC 27005, optymalną ze względu na charakter urzędu. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej metodyki analizy ryzyka, a Wykonawca zobowiązany jest je uwzględnić. Ponadto Wykonawca zobowiązany jest do przeprowadzenia procesu szacowania ryzyka zgodnie z wybraną i zatwierdzoną przez Zamawiającego metodyką szacowania ryzyka,
   - 1.2. Opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk,
   - 1.3. Przeszkolić kadrę zarządzającą urzędu w zakresie przyjętej metodyki szacowania ryzyka,
   - 1.4. Przeprowadzić wspólnie z wytypowanymi pracownikami urzędu proces szacowania ryzyka, a w szczególności:
     - 1.4.1. Zinwentaryzować zasoby na podstawie przekazanej przez Zamawiającego dokumentacji i ewentualnych dodatkowych koniecznych audytów (aktywa informacyjne) oraz ich właścicieli,
     - 1.4.2. Określić zagrożenia dla zasobów,
     - 1.4.3. Określić podatności dla zasobów,
     - 1.4.4. Określić skutki utraty poufności, integralności i dostępności zasobów,
     - 1.4.5. Przeanalizować i ocenić zidentyfikowane ryzyka.
   - 1.5. Opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Starostwa Powiatowego w Zakopanem,
   - 1.6. Opracować przy współudziale wytypowanych pracowników urzędu plan postępowania z ryzykiem,
   - 1.7. Przekazać Zamawiającemu narzędzia informatyczne wspomagające kontynuowanie procesu szacowania ryzyka w kolejnych okresach.

2. Wykonawca ma przekazać dokumentację, tj. metodykę szacowania ryzyka, raport z procesu szacowania ryzyka oraz plan postępowania z ryzykiem. Wykonawca przekaże Zamawiającemu w postaci dokumentacji elektronicznej na CD/DVD oraz papierowej. Forma elektroniczna dokumentacji będzie przygotowana w plikach edytowalnych.
3. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanej przez Wykonawcę dokumentacji. Wykonawca zobowiązany jest do uwzględnienia w dokumentacji wniesionych przez Zamawiającego uwag.
4. Produkty zadania:
   4.1. Metodyka szacowania ryzyka dla aktywów Zamawiającego w postaci dokumentacji elektronicznej na CD/DVD oraz papierowej

Opracowanie zaleceń

1. Wykonawca opracuje i przekaże Zamawiającemu dokument zalecanych modyfikacji w zakresie zabezpieczania informacji mających na celu osiągnięcie zgodności z wymaganiami normy ISO/IEC 27001
2. Produkty zadania:
   2.1. Dokumentacja zawierająca zalecenia modyfikacji w zakresie zabezpieczenia informacji zgodnie z wymaganiami normy ISO/IEC 27001

Etap 3 – Opracowanie dokumentacji PBI

1. Wykonawca na podstawie wyników uzyskanych w trakcie realizacji audytu, procesu klasyfikacji informacji oraz szacowania ryzyka zobowiązany jest opracować i przedstawić koncepcję wdrożenia Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Zakopanem.
   Koncepcja będzie w szczególności zawierać mapę dokumentów PBI, stanowiącą szczegółowy wykaz dokumentów PBI z zaznaczeniem ich wzajemnych powiązań w tym:
   1.1. Dokument Główny Polityki Bezpieczeństwa Informacji definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa w proces zapewnienia bezpieczeństwa informacji, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji,
   1.2. Polityka bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji w organizacji:
      1.2.1. Regulamin Ochrony Danych Osobowych,
      1.2.2. Plan Ciągłości Działania (BCP),
      1.2.3. Instrukcja bezpiecznego administrowania systemami teleinformatycznymi,
      1.2.4. Listy wymagań minimalnych dla głównych klas aktywów,
      1.2.5. Instrukcja bezpiecznego użytkowania systemów teleinformatycznych,
      1.2.6. Procedura okresowych wewnętrznych audytów bezpieczeństwa,
      1.2.7. Plan audytów wewnętrznych i zewnętrznych,
      1.2.8. Instrukcje sporządzania cyklicznych raportów dla właścicieli kluczowych aktywów i kadry zarządzającej,
      1.2.9. Procedury eksploatacyjne dla głównych klas aktywów,
      1.2.10. Szablony rejestrów oraz upoważnień przewidzianych w regulaminach, instrukcjach i procedurach.

1.3. Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji, w tym tabele odpowiedzialności pracowników – RACI,
1.4. Procedury bezpieczeństwa i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z regulaminów bezpieczeństwa obszarów, o których mowa w pkt 1.2 oraz potrzebnych do przejścia procesu certyfikacji,
1.5. Opracowanie formularzy i rejestrów będących integralną częścią w/w dokumentów w formie i treści odpowiedniej do potrzeb i woli Zamawiającego.
1.6. Opracowanie katalogu świadczonych usług informatycznych oraz przydzieloną odpowiedzialnością pracowników za usługę (model RACI) wraz z dokumentacją implementującą wybrane elementy dobrych praktyk ITIL (Information Technology Infrastructure Library) lub normy PN-ISO/IEC 20000 w środowisku IT urzędu. Katalog świadczonych usług informatycznych będzie zawierał listę usług w podziale na kategorie oraz ich opis z perspektywy klientów/użytkowników usług, z podaniem dostępnych poziomów wsparcia oraz odpowiedzialności pracowników za usługę według modelu RACI (Responsible, Accountable, Contribution, Informed).

2. Produkty zadania:
2.1. Dokumentacja koncepcyjna Polityki bezpieczeństwa Starostwa Powiatowego w Zakopanem wraz z wszystkimi dokumentami towarzyszącymi do zatwierdzenia przez Zamawiającego.
3. Dla każdego dokumentu, o którym mowa w pkt. 1. Wykonawca opracuje i przedstawi do akceptacji szczegółowy zakres merytoryczny. W przypadku dokumentów funkcjonujących w Starostwie Powiatowym w Zakopanem odnoszących się do bezpieczeństwa informacji, których zakres merytoryczny będzie w całości lub częściowo pokrywał się z opracowanymi przez Wykonawcę projektami dokumentów PBI, Wykonawca zaproponuje i uzasadni sposób ich, wyłączenia, zastąpienia lub zintegrowania z zaproponowaną przez Wykonawcę mapą dokumentów.
4. Zamawiający zastrzega sobie prawo do wnoszenia uwag do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego. Uwagi wnoszone przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji wdrożenia PBI.
5. Na podstawie zatwierdzonej przez Zamawiającego koncepcji, o której mowa w pkt. 1., Wykonawca opracuje wszystkie opisane w koncepcji dokumenty Polityki Bezpieczeństwa Informacji Starostwa Powiatowego w Zakopanem uwzględniając wszystkie uwagi zamawiającego.
5.1. Dokumenty PBI, o których mowa w pkt. 4. muszą być zgodne ze wszystkimi wymaganiami prawnymi, którymi podlega Starostwo Powiatowe w Zakopanem, w szczególności – w zakresie bezpieczeństwa informacji i ochrony danych osobowych, oraz z wymaganiami normy ISO 27001. Jeżeli w trakcie realizacji umowy wymagania prawne w zakresie bezpieczeństwa informacji ulegną zmianie, Wykonawca zobowiązany jest dostosować dokumentację PBI do zaistniałych zmian (np. RODO).
5.2. Wszystkie dokumenty Polityki Bezpieczeństwa Informacji, Wykonawca przekaże Zamawiającemu w formie dokumentacji elektronicznej na CD/DVD oraz w formie papierowej. Forma elektroniczna dokumentacji będzie przygotowana w plikach edytowalnych.
5.3. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów PBI, o których mowa w pkt. 4.

5.4. Wykonawca jest zobowiązany do wprowadzenia zmian w dokumentach PBI zgodnie z uwagami Zamawiającego, o których mowa w pkt 7.

6. Produkty zadania:
   6.1. Komplet dokumentacji „Polityka Bezpieczeństwa Informacji Starostwa Powiatowego w Zakopanem”
      6.1.1. Nie zawierająca informacji i powiązań informacji będących przedmiotem ochrony. Stworzona w taki sposób, aby można było ją ujawniać, a wszelkie informacje szczegółowe wskazane były w dokumentach towarzyszących, niejawnych,
      6.1.2. określająca cele i wytyczne dbałości o bezpieczeństwo informacji,
      6.1.3. powołujący organizację bezpieczeństwa informacji,
      6.1.4. wskazujący na dokumenty szczegółowe, definiujące zasady i działania, o których wiedza nie powinna być ogólnie dostępna.

Etap 4 – Wdrożenie i zapoznanie pracowników z powstałej Polityki Bezpieczeństwa Informacji

1. Wykonawca zobowiązany jest do udostępnienia PBI oraz jej dokumentów w wersji elektronicznej dla pracowników Starostwa Powiatowego w Zakopanem celem zapoznania się z dokumentacją przez pracowników urzędu. Dokumentacja powinna być wyłącznie w trybie przeglądania oraz pliki zabezpieczone przed kopiowaniem.
2. W Wykonawca zobowiązany jest do przygotowania i poprowadzenia szkoleń ze stworzonej i zatwierdzonej przez Zamawiającego Polityki Bezpieczeństwa Informacji dla pracowników Starostwa Powiatowego w Zakopanem.
   2.1. Szkolenia dla pracowników będą obejmowały swoim zakresem co najmniej:
      2.1.1. Omówienie podstawowych zasad bezpieczeństwa informacji, wynikających z PBI,
      2.1.2. Odpowiedzialność za naruszenie zasad PBI,
      2.1.3. Zasady zgłaszania i reagowania na incydenty,
   2.2. Szkolenia dla pracowników zostaną przeprowadzone dla trzech grup.
   2.3. Szkolenie dla każdej z grup pracowników będzie trwało co najmniej 2 godziny zegarowe.
   2.4. Szkolenia dla pracowników będą odbywały się w siedzibie Zamawiającego w dni robocze pomiędzy godziną 8:00 a 15:15.
3. Wykonawca przygotuje i poprowadzi również warsztaty dla koordynatora bezpieczeństwa, audytorów wewnętrznych i trenerów PBI.
   3.1. Warsztaty dla audytorów wewnętrznych PBI będzie obejmowało swoim zakresem co najmniej:
      3.1.1. Zasady audytowania PBI,
      3.1.2. Monitorowanie skuteczności PBI,
      3.1.3. Opracowanie wyników z audytu wewnętrznego (działania korygujące, działania, zapobiegawcze).
   3.2. Celem warsztatów dla trenerów będzie zdobycie przez uczestników warsztatów wiedzy, umożliwiającej wykonywanie nowych obowiązków oraz prowadzenie szkoleń z PBI dla pracowników Starostwa Powiatowego w Zakopanem.
   3.3. Warsztaty dla koordynatora bezpieczeństwa, audytorów wewnętrznych i trenerów PBI będzie przeprowadzone dla grupy około 5 - ciu osób oraz będzie trwało przynajmniej 1 dzień roboczy.

3.4. Warsztaty dla koordynatora bezpieczeństwa, audytorów wewnętrznych i trenerów PBI będą odbywać się w siedzibie Zamawiającego.
3.5. Wykonawca przekaże do akceptacji Zamawiającemu harmonogram warsztatów, materiały dydaktyczne i prezentacje najpóźniej na 7 dni przed planowanym terminem rozpoczęcia warsztatów.
3.6. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanych przez Wykonawcę materiałów dydaktycznych i harmonogramu warsztatów, w tym do zmiany planowanych terminów warsztaów. Wykonawca zobowiązany jest do uwzględnienia uwag.

4. Wykonawca zapewni jeden kurs dla audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001:2013 wg Akredytacji IRCA A17287 oraz będzie trwał przynajmniej 5 dni roboczych.
4.1. Niniejszy kurs może się odbyć poza siedzibą urzędu.
4.2. Wykonawca ma zapewnić, że kurs o którym w pkt. 4 zakończy się egzaminem sprawdzającym nabytą wiedzę i umiejętności przez uczestnika kursu.
5. W ramach realizowanej usługi Wykonawca przygotuje szkolenie e-learningowe z Polityki Bezpieczeństwa Informacji, które posłuży jako materiał szkoleniowy dla pracowników Starostwa Powiatowego w Zakopanem.
5.1. Wykonawca dostarczy platformę e-learningową oraz ją zainstaluje na wskazanych przez Zamawiającego serwerach urzędu.
5.2. Wykonawca jest zobowiązany do opracowania programu szkolenia e-learningowego zgodnie z przyjętą Polityką Bezpieczeństwa Informacji oraz z wymaganiami Zamawiającego.
5.3. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę programu szkolenia e-learningowego. Wykonawca zobowiązany jest do uwzględnienia uwag.
6. Wykonawca zobowiązany jest ponadto do przygotowania i przedłożenia Zamawiającemu:
6.1. Imiennej listy obecności uczestników szkolenia sporządzanej odrębnie dla każdego dnia szkolenia, zawierającej: informacje o liczbie godzin, obecności danej osoby, podpis uczestnika szkolenia, podpis wykładowcy/wykładowców.
6.2. Zamawiający zastrzega sobie prawo do rejestracji audio-wizualnej przebiegu szkoleń.
6.3. Wykonawca zobowiązany jest wystawić wszystkim osobom biorącym udział w szkoleniu imienny certyfikat uczestnictwa w szkoleniu.
7. Produkty zadania:
7.1. Materiały dydaktyczne
7.2. Materiały e-learningowe

Etap 4 – Audyt powdrożeniowy

1. Audyt powdrożeniowy będzie obejmował następujące prace:
1.1. Weryfikację poziomu wdrożenia w Starostwie Powiatowym w Zakopanem zabezpieczeń zgodnie z rekomendacjami, o których mowa w pkt 2.7.1.5 dotyczącym Audytu zasadniczego.
1.2. Weryfikację stosowania zasad określonych w Polityce Bezpieczeństwa Informacji przez pracowników urzędu.

1.3. Ocenę poziomu spełnienia wymagań normy PN-ISO/IEC 27001 zgodnie z załącznikiem A do niniejszej normy.

2. Wykonawca zobowiązany jest przedstawić Zamawiającemu szczegółowy plan audytu, który będzie podlegał akceptacji przez Zamawiającego.
3. Wykonawca zobowiązany jest opracować raport z audytu powdrożeniowego zawierający co najmniej:
   3.1. Cel i zakres przeprowadzonego audytu,
   3.2. Szczegółowy opis przeprowadzonych prac,
   3.3. Szczegółowy opis poziomu spełnienia wymagań normy PN-ISO/IEC 27001, w obszarach, w których podczas audytu przedwdrożeniowego stwierdzono niezgodności,
   3.4. Wykaz zaobserwowanych niezgodności w odniesieniu do stosowania przez pracowników urzędu zasad Polityki Bezpieczeństwa Informacji,
   3.5. Szczegółowy opis działań korygujących i naprawczych,
   3.6. Ogólną ocenę poziomu spełnienia wymagań normy PN-ISO/IEC 27001 zgodnie z załącznikiem A do niniejszej normy oraz poziomu stosowania przez pracowników Starostwa Powiatowego w Zakopanem zasad Polityki Bezpieczeństwa Informacji,
   3.7. Podsumowanie i wnioski.
4. Zamawiający na podstawie niezgodności ujętych w raporcie, podejmie działania w oparciu o wydane rekomendacje prowadzące do spełnienia wymagań normy PN-ISO/IEC 27001.
5. Wykonawca po zapewnieniu przez Zamawiającego o usuniętych niezgodnościach, przeprowadzi w tym zakresie powtórny audyt sprawdzający spełnienie wymagań normy PN-ISO/IEC 27001 przez Zamawiającego.
6. W przypadku spełnienia wymagań normy PN-ISO/IEC 27001 przez Zamawiającego na podstawie wykonanego audytu, Wykonawca wystawi dokument poświadczający spełnienie wymagań normy PN-ISO/IEC 27001.
7. Najważniejsze wnioski z audytu powdrożeniowego Wykonawca jest zobowiązany przedstawić kierownictwu urzędu w formie prezentacji multimedialnej.
8. Raport, o którym mowa w punkcie 3 Wykonawca przekaże Zamawiającemu w formie elektronicznej oraz papierowej. Forma elektroniczna raportu, będzie przygotowana w plikach edytowalnych.
9. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu, o którym mowa w pkt 8. Wykonawca zobowiązany jest do uwzględnienia w wyżej wymienionym raporcie wniesionych przez Zamawiającego uwag.
10. Produkty zadania:
    10.1. Raport z audytu powdrożeniowego
    10.2. Dokument poświadczający spełnienie wymagań normy PN-ISO/IEC 27001
11. Wykonawca udziela Zamawiającemu gwarancji na system zarządzania zgodnego z normą ISO/IEC 27001, zwanego dalej systemem, która obejmuje pozytywne przejście procesu certyfikacji systemu, w jednostce certyfikującej systemy zarzadzania na zgodność z normą ISO/IEC 27001, akredytowanej przez dowolną jednostką akredytującą wymienioną na stronie http://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4.

Audyt bezpieczeństwa systemów teleinformatycznych

1. Wykonawca przeprowadzi audyt bezpieczeństwa systemów teleinformatycznych obejmujący audyt bezpieczeństwa Zintegrowanego Geodezyjnego Systemu Informatycznego wraz z

Geoportalem udostępniającym e-usługi oraz audyt aktywów z nim powiązanych polegający na praktycznej analizie zabezpieczeń systemu teleinformatycznego w postaci:

1.1. Punktów styku siecią,
1.2. Punktów węzłowych sieci,
1.3. Serwerów,
1.4. Urządzeń końcowych w Wydziale Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami oraz administratorów systemów informatycznych

2. W ramach audytu Wykonawca wykona:
   2.1. Testy penetracyjne z poziomu sieci lokalnej i Internetu
   2.2. Testy bezpieczeństwa sieci bezprzewodowej
   2.3. Skanowanie systemów pod kątem luk bezpieczeństwa
   2.4. Badanie bezpieczeństwa systemów webowych (serwisów i stron www) w szczególności Geoportalu udostępniającego e-usługi
   2.5. Badanie odporności użytkowników na socjotechniki
3. Celem audytu jest praktyczna ocenę bieżącego stanu bezpieczeństwa systemu, w szczególności podatności i odporności na próby przełamania zabezpieczeń
4. Audyt penetracyjny polega na analizie systemu i jego zabezpieczeń pod kątem:
   4.1. Potencjalnych błędów bezpieczeństwa spowodowanych niewłaściwą konfiguracją,
   4.2. Lukami w oprogramowaniu,
   4.3. Lukami w sprzęcie,
   4.4. Słabościami w technicznych,
   4.5. Słabościami proceduralnymi,
   4.6. Poziomem świadomości użytkowników.
5. Wykonawca zobowiązany jest przedstawić Zamawiającemu szczegółowy plan audytu, który będzie podlegał akceptacji przez Zamawiającego.
6. Wykonawca zobowiązany jest opracować raport z audytu bezpieczeństwa systemów teleinformatycznych zawierający co najmniej:
   6.1. Cel i zakres przeprowadzonego audytu,
   6.2. Szczegółowy opis przeprowadzonych prac,
   6.3. Szczegółowy opis poziomu stanu zabezpieczeń środowiska teleinformatycznego,
   6.4. Opis zabezpieczeń jakie należy wdrożyć,
   6.5. Informacje o lukach bezpieczeństwa jakie należy wyeliminować
   6.6. Podsumowanie i wnioski
7. Raport, o którym mowa w punkcie 6 Wykonawca przekaże Zamawiającemu w formie elektronicznej oraz papierowej. Forma elektroniczna raportu, będzie przygotowana w plikach edytowalnych.