Cyberbezpieczny Samorząd

Biała, 25 listopada 2024 r.

Znak IR.IFS.041.30.1.2023

Gmina Stara Biała
ul. Jana Kazimierza 1
09-411 Biała

Zapytanie ofertowe

przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa
dla kadry kierowniczej, pracowników Urzędu Gminy Stara Biała i jednostek organizacyjnych Gminy

o wartości nie przekraczającej wyrażonej w złotych równowartości kwoty określonej
w art. 2 ust. 1 pkt 1) ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych
(tekst jednolity Dz.U. z 2024 poz. 1320 z późn. zm.).

1. Nazwa i dane adresowe Zamawiającego

Zamawiający:	Gmina Stara Biała
Adres:	ul. Jana Kazimierza 1, 09-411 Biała
Telefon:	+48 24 366 87 10
E-mail:	gmina@starabiala.pl
	a.kozlowska@starabiala.pl
Strona internetowa:	https://www.starabiala.pl/
Strona BIP:	https://bip.starabiala.pl//
NIP:	774 294 52 31
REGON:	611016028

2. Wstęp

Zamówienie jest realizowane w ramach grantu w projekcie grantowym **„Cyberbezpieczny Samorząd”** współfinansowanym przez Unię Europejską z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: *Zaawansowane usługi cyfrowe*, Działanie 2.2. – *Wzmocnienie krajowego systemu cyberbezpieczeństwa*, na podstawie umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1524/ FERC.02.02-CS.01-001/23/2024 z dnia 29 maja 2024 r. W ramach projektu przewidziano kompleksowe przeszkolenie z zakresu cyberbezpieczeństwa w celu zapewnienia regularnego podnoszenia poziomu świadomości cyberbezpieczeństwa u wszystkich pracowników Urzędu Gminy Stara Biała i jednostek organizacyjnych Gminy („Urząd”).

3. TRYB UDZIELENIA ZAMÓWIENIA:

1. Na podstawie art. 2 ust. 1 pkt. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych niniejsze postępowanie nie podlega przepisom ww. ustawy.
2. Oznaczenie wg Wspólnego Słownika Zamówień (kod CPV):
   80533100-0 usługi szkolenia komputerowego
3. Zamawiający dopuszcza składanie ofert częściowych.
4. Zamawiający nie dopuszcza składania ofert wariantowych.
5. Zamawiający nie przewiduje udzielania zamówień uzupełniających.
6. Postępowanie prowadzone jest w języku polskim, w portalu Baza Konkurencyjności: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl

4. Wymagania ogólne (do wszystkich części zamówienia)

We wszystkich częściach zamówienia muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępność dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn. W przypadku szkoleń online, wymagane będzie spełnienie przez wykonawcę wymogów dostępności oraz WCAG 2.1 dla narzędzi, które zostaną wykorzystane do szkoleń w zależności od potrzeb uczestników szkolenia). W ramach grup szkoleniowych przewidziana jest równa dostępność dla kobiet i mężczyzn oraz osób niepełnosprawnych. Opracowane materiały szkoleniowe będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści.

Wykonawca każdej z części zamówienia będzie zobowiązany do podpisania oświadczenia potwierdzającego przestrzeganie powyższych zasad.

5. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest przeprowadzenie w formule on-line szkoleń z zakresu cyberbezpieczeństwa dla kadry kierowniczej, pracowników Urzędu Gminy Stara Biała i jednostek organizacyjnych.

Przedmiot zamówienia jest podzielony na 11 części. Ocena ofert zostanie przeprowadzona odrębnie dla każdej części. Wykonawcy mogą składać oferty na dowolną liczbę części.

Szkolenia (części 1. – 11. zamówienia) muszą spełniać następujące wymagania:

1. Miejscem realizacji zamówienia jest:
   a. Siedziba Urzędu Gminy Stara Biała, ul. Jana Kazimierza 1, 09-411 Biała.
   b. Siedziba Szkoły Podstawowej im Jana Pawła II, Stara Biała, 53, 09-411 Biała
   c. Siedziba Zespołu Szkolno-Przedszkolnego w Wyszynie, Wyszyna 2, 09-411 Biała
   d. Siedziba Szkoły Podstawowej w Starych Proboszczewicach, ul. Floriańska 4, 09-412 Proboszczewice
   e. Siedziba Przedszkola w Nowych Proboszczewicach, ul. Floriańska 20, 09-412 Proboszczewice
   f. Siedziba Szkoły Podstawowej im. Władysława Stanisława Reymonta w Maszewie Dużym, ul. Szkolna 14,

09 - 400 Maszewo Duże

g. Siedziba Gminnego Ośrodka Pomocy Społecznej, ul. Jana Kazimierza 1,09-411 Biała

2. Szkolenia muszą odbywać się w godzinach pracy Urzędu oraz jednostek organizacyjnych.
3. Wykonawca w ramach wykonania usługi przedstawi szczegółowy program szkolenia zawierający informacje dotyczące tematyki i czasu szkolenia, i dostarczy go w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji Zamawiającego.
4. Opracowane materiały będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści. W ramach wynagrodzenia Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia. Zamawiający dopuszcza dostarczenie kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF.
5. Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia.
6. W ramach wynagrodzenia Wykonawca dostarczy Zamawiającemu materiały ze szkolenia, które to będzie mógł wykorzystać do przeszkolenia osób nieobecnych lub nowoprzyjętych.
7. Wykonawca nie jest zobowiązany do zapewnienia uczestnikom wyżywienia podczas szkoleń on - line.
8. Każdy uczestnik szkolenia otrzyma od Wykonawcy imienny certyfikat z podpisem trenera, potwierdzający ukończenie szkolenia i jego zakres.
9. Zamawiający zwraca uwagę, że szkolenia będące przedmiotem zamówienia mają charakter kształcenia zawodowego i są finansowane w całości ze środków publicznych, w związku z czym są one zwolnione z podatku od towarów i usług na podstawie §3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 roku w sprawie zwolnień od podatku towarów i usług oraz warunków stosowania tych zwolnień (t.j. Dz.U. 2023 poz. 955).

5.1. Część 1.: Cyberbezpieczeństwo dla kadry kierowniczej oraz działu IT z podstawami prawnymi dla Urzędu Gminy Stara Biała

W ramach realizacji części 1. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego dla kadry kierowniczej w zakresie bezpieczeństwa informacji i wymogów w zakresie cyberbezpieczeństwa. Celem szkolenia jest zwiększenie świadomości kadry kierowniczej Urzędu w zakresie problematyki związanej z bezpieczeństwem informacji, rozwinięcie umiejętności strategicznego zarządzania cyberbezpieczeństwem oraz zrozumienie przepisów prawnych i ich implementacji.

Szkolenie musi obejmować co najmniej następującą tematykę:

1.podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania),

2.przegląd najpopularniejszych zagrożeń (w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa),

3.znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego,

4.przegląd aktualnych zagrożeń i trendów w cyberprzestrzeni,

5.analiza przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773) i ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077),

6.cyberbezpieczeństwo jednostki samorządu terytorialnego w kontekście bezpieczeństwa państwa,

7.zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w cyberprzestrzeni,

8.obowiązki jednostek samorządu terytorialnego wynikające z przepisów,

9.metody identyfikacji i oceny ryzyka,

10.tworzenie i implementacja polityk ochrony danych,

11.standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie, cyberhigiena,

12.procesy i procedury zarządzania incydentami oraz role poszczególnych pracowników,

13.rola kadry kierowniczej w zakresie cyberbezpieczeństwa (w tym w sytuacjach kryzysowych),

14.incydenty w kontekście zachowania ciągłości działania urzędu,

15.przywództwo, motywowanie zespołu i promocja kultury bezpieczeństwa w urzędzie.

W wyniku szkolenia kadra kierownicza musi być w stanie efektywnie zarządzać cyberbezpieczeństwem w urzędzie, podejmować strategiczne decyzje dotyczące ochrony danych oraz promować kulturę bezpieczeństwa wśród pracowników. Dzięki temu urząd będzie lepiej przygotowany na ewentualne zagrożenia i incydenty.

Wymagana forma przeprowadzenia szkolenia: szkolenie grupowe w formule on-line. Zamawiający zapewni pomieszczenie i komputer, rzutnik oraz łącze internetowe do przeprowadzenia szkolenia.

Liczba osób do przeszkolenia – 11

Czas trwania szkolenia – 5 godzin

Liczba edycji szkolenia – 1 (planowany termin rok 2024 lub 2025).

Program szkolenia może zostać zmodyfikowany i musi odnosić się do aktualnych aktów prawnych, zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków obrony przed nimi.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.2. Część 2.: System Zarządzania Ciągłością Działania w bezpieczeństwie informacji w aspekcie kadry kierowniczej w Urzędzie Gminy Stara Biała

W ramach realizacji części 2. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **szkolenia w formule on -line** dla kadry kierowniczej w Urzędzie Gminy Stara Biała budującego świadomość cyberzagrożeń i sposobów ochrony. Celem szkolenia jest budowa świadomości i umiejętności praktycznych w zakresie budowania procedur oraz zarządzania ciągłością działania w bezpieczeństwie informacji, strategii ciągłości, kontekstu jednostki, Polityki Ciągłości Działania.

Szkolenie musi obejmować co najmniej następującą tematykę:
Niezbędne przepisy, wytyczne oraz standardy celem prawidłowego zrozumienia zarządzania ciągłością działania.

1. Podstawy prawne dla ciągłości: RODO / KRI / KSC.
2. Wspólne elementy RODO / KRI / KSC z ciągłością działania.
3. Zjawisko ciągłości działania oraz systemu zarządzania.
4. Cykl Deminga (PDCA).
5. Omówienie założeń ISO oraz standardów z rodziny norm 27xxx, 29xxx, 31xxx oraz norm audytujących.
6. Normy ISO jako standardy lub wymogi prawne
7. Rodzaje audytów, audytorów (i ich uprawnienia) oraz wymogi wykonywania audytów w różnych przepisach prawa.
8. Ciągłość działania: techniki audytowania oraz sytuacje, podczas których audyt jest wymagany.
9. Definicje legalne / słownik pojęć w Zarządzaniu Ciągłością Działania ze szczegółowym wyjaśnieniem.
10. Budowa dokumentacji SZCD w oparciu o polski standard ISO 22301 ze szczególnym uwzględnieniem stosowania cyklu Deminga – cz. 1. Obszar: kontekst organizacji, przywództwo, planowanie oraz wsparcie.
11. Budowa dokumentacji SZCD w oparciu o polski standard ISO 22301 ze szczególnym uwzględnieniem stosowania cyklu Deminga – cz. 2. Obszar: działania operacyjne, ocena efektów działania oraz doskonalenie.
12. Szczegółowe omówienie zjawiska Analizy wpływu biznesowego (BIA) (Analizy wpływu na kluczowe procesy).
13. Szczegółowe omówienie oceny ryzyka w zakresie ciągłości działania. Różnica pomiędzy „oceną ryzyka” w ciągłości działania a „oceną ryzyka” w bezpieczeństwie informacji.
14. Plany Ciągłości Działania – budowa oraz sposób ich tworzenia w oparciu o ustandaryzowane katalogi zagrożeń.
15. Omówienie praktycznych wskazówek Zarządzania Ciągłością Działania w obszarze formalnoprawnym oraz informatycznym.

Wymagana forma przeprowadzenia szkolenia: **szkolenie grupowe w formule on-line.** Zamawiający zapewni salę szkoleniową z komputerem, rzutnikiem.

Liczba osób do przeszkolenia – 11

Czas trwania szkolenia – min. 5 godzin

Liczba edycji szkolenia – 1 (planowany termin rok 2024 lub 2025).

Program szkolenia może zostać zmodyfikowany i musi odnosić się do aktualnych zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków obrony przed nimi.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.3. Część 3.: Szacowanie ryzyka bezpieczeństwa informacji – ryzyko ogólne oraz utraty praw i wolności osób fizycznych w aspekcie kadry kierowniczej w Urzędzie Gminy Stara Biała

W ramach realizacji części 3. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **szkolenia specjalistycznego** dla kadry kierowniczej w zakresie szacowania bezpieczeństwa informacji i wymogów w zakresie cyberbezpieczeństwa. Celem szkolenia jest zwiększenie świadomości kadry kierowniczej Urzędu Gminy Stara Biała w zakresie metodologii szacowania ryzyka (do wdrożenia w Systemie Zarządzania Bezpieczeństwem Informacji (Polityki)), oprogramowania do szacowania ryzyka wobec zagrożeń występujących podczas pracy zdalnej.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Omówienie niezbędnych przepisów celem prawidłowego zrozumienia procesu szacowania ryzyka w kontekście RODO, rozporządzenia Krajowych Ram Interoperacyjności, norm ISO oraz Kodeksu Pracy.
2. Omówienie zjawiska pracy zdalnej w oparciu o aktualnie obowiązujące przepisy prawa w zakresie bezpieczeństwa informacji.
3. Analiza stosowanych aktywów oraz występujących zagrożeń w kontekście standardów ISO.
4. Wskazanie międzynarodowych norm ISO pomocnych w procesie szacowania ryzyka.
5. Wskazanie niezbędnych elementów składających się na szacowanie ryzyka podczas pracy zdalnej. Szczegółowa analiza katalogu 35 najczęściej występujących zagrożeń z uwzględnieniem podziału na 7 kategorii, 3 atrybutów bezpieczeństwa informacji oraz stosowanych aktywów. Omówienie autorskich zaleceń wobec zagrożeń.
6. Proces klasyfikacji czynności przetwarzania zidentyfikowanych w jednostce/organizacji w kontekście pracy zdalnej.
7. Omówienie skali podatności, skutku i ryzyka (+ zaznaczenie różnicy pomiędzy szacowaniem jakościowym i

ilościowym).

8. Proces etapu oceny ryzyka w szacowaniu ryzyka – praca z macierzą (w oparciu o autorskie rozwiązanie ISO-LEX).
9. Omówienie filozofii działania na macierzach ryzyka.
10. Zasady postępowania z ryzykiem.
11. Przygotowanie planu postępowania z ryzykiem

Wymagana forma przeprowadzenia szkolenia: szkolenie grupowe w formule on-line. Zamawiający zapewni salę szkoleniową z komputerem, rzutnikiem.

Liczba osób do przeszkolenia – 11

Czas trwania szkolenia – min. 5 godzin

Liczba edycji szkolenia – 1 (planowany termin rok 2024 lub 2025).

Program szkolenia może zostać zmodyfikowany i musi odnosić się do aktualnych zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków obrony przed nimi.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.4. Część 4.: Wymogi wynikające z Rozporządzenia KRI, Ustawy o KSC oraz RODO, po zmianach wynikających z wdrożenia Dyrektywy NIS 2

W ramach realizacji części 4. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **szkolenia specjalistycznego** dla kadry kierowniczej w zakresie Krajowych Ram Interoperacyjności (KRI) w bezpieczeństwie informacji, na podstawie czego powstały i z jakimi przepisami się łączą, jakie procedury wynikają z KRI, czy są one wystarczająco wskazane. Ponadto uczestnicy szkolenia uzyskają wiedzę jak zbudować dokumentację w oparciu o art. 25 RODO. Co składa się na dokumentację z zakresu ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Omówienie niezbędnych przepisów celem prawidłowego zrozumienia KRI.
2. Wymogi KRI w zakresie dokumentacji, procedur i zabezpieczeń, oraz ich omówienie.
3. Omówienie zasad szkoleń, audytów i kontroli. Kto i kogo kontroluje, audytuje oraz szkoli.
4. Omówienie podstawowych zagadnień oraz pojęć odnoszących się do KRI.
5. Wskazanie międzynarodowych norm ISO pomocnych przy realizacji założeń KRI.
6. Przesłanki determinujące przeprowadzenie audytu KRI.
7. Warstwowość KRI: sposoby osiągania interoperacyjności.

8. Rodzaje audytów oraz audytorów.
9. Różnica pomiędzy audytem KRI (Krajowych Ram Interoperacyjności) a audytem KSC (Krajowego Systemu Cyberbezpieczeństwa).
10. Wprowadzenie do art. 25 RODO - czym jest „Privacy by design" oraz „Privacy by default".
11. Wytyczne EROD-u nr 4/2019 dotyczące art. 25 RODO.
12. Rozliczalność dla art. 25 RODO.
13. Praktyczne aspekty tworzenia dokumentacji z zakresu ochrony danych osobowych w fazie projektowania oraz domyślnej ochrony danych.
14. Wdrażanie dokumentacji z zakresu ochrony danych osobowych w fazie projektowania oraz domyślnej ochrony danych, a także weryfikacja takiej dokumentacji.

Wymagana forma przeprowadzenia szkolenia: **szkolenie grupowe w formule on-line.** Zamawiający zapewni salę szkoleniową z komputerem, rzutnikiem.

Liczba osób do przeszkolenia – 11

Czas trwania szkolenia – min. 5 godzin

Liczba edycji szkolenia – 1 (planowany termin rok 2024 lub 2025).

Program szkolenia może zostać zmodyfikowany i musi odnosić się do aktualnych zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków obrony przed nimi.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.5. Część 5.: Cyberbezpieczeństwo w praktyce sektora realizującego zadania publiczne dla pracowników Urzędu Gminy Stara Biała oraz jednostek organizacyjnych Gminy

W ramach realizacji części 5. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego dla pracowników Urzędu Gminy Stara Biała w zakresie bezpieczeństwa informacji i wymogów w zakresie cyberbezpieczeństwa. Celem szkolenia jest zwiększenie świadomości pracowników Urzędu w zakresie problematyki związanej z bezpieczeństwem informacji, rozwinięcie umiejętności strategicznego zarządzania cyberbezpieczeństwem oraz zrozumienie przepisów prawnych i ich implementacji.

Szkolenie musi obejmować co najmniej następującą tematykę:

1.Podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania),

2.Przegląd najpopularniejszych zagrożeń (w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo

na dyrektora/prezesa),

3.Znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego,

4.Przegląd aktualnych zagrożeń i trendów w cyberprzestrzeni,

5.Analiza przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773) i ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077),

6.Cyberbezpieczeństwo jednostki samorządu terytorialnego w kontekście bezpieczeństwa państwa,

7.Zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w cyberprzestrzeni,

8.Obowiązki jednostek samorządu terytorialnego wynikające z przepisów,

9.Metody identyfikacji i oceny ryzyka,

10.Tworzenie i implementacja polityk ochrony danych,

11.Standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie, cyberhigiena,

12.Procesy i procedury zarządzania incydentami oraz role poszczególnych pracowników,

13.Incydenty w kontekście zachowania ciągłości działania urzędu,

14.Przywództwo, motywowanie zespołu i promocja kultury bezpieczeństwa w urzędzie.

W wyniku szkolenia kadra kierownicza musi być w stanie efektywnie zarządzać cyberbezpieczeństwem w urzędzie, podejmować strategiczne decyzje dotyczące ochrony danych oraz promować kulturę bezpieczeństwa wśród pracowników. Dzięki temu urząd będzie lepiej przygotowany na ewentualne zagrożenia i incydenty.

Wymagana forma przeprowadzenia szkolenia: **szkolenie grupowe w formule on-line.** Zamawiający zapewni pomieszczenie i komputer, rzutnik oraz łącze internetowe do przeprowadzenia szkolenia.

Liczba osób do przeszkolenia:

a. Urząd Gminy Stara Biała - 31

b. Szkoła Podstawowa im Jana Pawła II w Starej Białej - 34

c. Zespół Szkolno-Przedszkolny w Wyszynie - 58

d. Szkoła Podstawowa w Starych Proboszczewicach - 58

e. Przedszkole w Nowych Proboszczewicach - 35

f. Szkoła Podstawowa im. Władysława Stanisława Reymonta w Maszewie Dużym - 73

g. Gminny Ośrodek Pomocy Społecznej - 14

Czas trwania szkolenia – 5 godzin

Liczba edycji szkolenia – 7 (planowany termin rok 2024 lub 2025).Program szkolenia może zostać zmodyfikowany i

musi odnosić się do aktualnych aktów prawnych, zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków o obrony przed nimi.

Program szkolenia może zostać zmodyfikowany i musi odnosić się do aktualnych zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków obrony przed nimi.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.6. Część 6.:Wymagania dla pracowników Urzędu Gminy Stara Biała oraz jednostek organizacyjnych gminy wynikające z Rozporządzenia KRI, Ustawy o KSC oraz RODO

W ramach realizacji części 6. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego dla pracowników Urzędu Gminy Stara Biała w zakresie Krajowych Ram Interoperacyjności (KRI) w bezpieczeństwie informacji, na podstawie czego powstały i z jakimi przepisami się łączą, jakie procedury wynikają z KRI, czy są one wystarczająco wskazane. Ponadto uczestnicy szkolenia uzyskają wiedzę jak zbudować dokumentację w oparciu o art. 25 RODO. Pracownicy Urzędu dowiedzą się co składa się na dokumentację z zakresu ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych.

Szkolenie musi obejmować co najmniej następującą tematykę:

1.Omówienie niezbędnych przepisów celem prawidłowego zrozumienia KRI.

2.Wymogi KRI w zakresie dokumentacji, procedur i zabezpieczeń, oraz ich omówienie.

3.Omówienie zasad szkoleń, audytów i kontroli. Kto i kogo kontroluje, audytuje oraz szkoli.

4.Omówienie podstawowych zagadnień oraz pojęć odnoszących się do KRI.

5.Wskazanie międzynarodowych norm ISO pomocnych przy realizacji założeń KRI.

6.Przesłanki determinujące przeprowadzenie audytu KRI.

7.Warstwowość KRI: sposoby osiągania interoperacyjności.

8.Rodzaje audytów oraz audytorów.

9.Różnica pomiędzy audytem KRI (Krajowych Ram Interoperacyjności) a audytem KSC (Krajowego Systemu Cyberbezpieczeństwa.

10.Wprowadzenie do art. 25 RODO - czym jest „Privacy by design” oraz „Privacy by default”.

11.Wytyczne EROD-u nr 4/2019 dotyczące art. 25 RODO.

12.Rozliczalność dla art. 25 RODO.

13.Praktyczne aspekty tworzenia dokumentacji z zakresu ochrony danych osobowych w fazie projektowania oraz domyślnej ochrony danych.

14.Wdrażanie dokumentacji z zakresu ochrony danych osobowych w fazie projektowania oraz domyślnej ochrony

danych, a także weryfikacja takiej dokumentacji.

Wymagana forma przeprowadzenia szkolenia: **szkolenie grupowe w formule on-line.** Zamawiający zapewni salę szkoleniową z komputerem, rzutnikiem.

Liczba osób do przeszkolenia:

a. Urząd Gminy Stara Biała - 31

b. Szkoła Podstawowa im Jana Pawła II w Starej Białej - 34

c. Zespół Szkolno-Przedszkolny w Wyszynie - 58

d. Szkoła Podstawowa w Starych Proboszczewicach - 58

e. Przedszkole w Nowych Proboszczewicach - 35

f. Szkoła Podstawowa im. Władysława Stanisława Reymonta w Maszewie Dużym - 73

g. Gminny Ośrodek Pomocy Społecznej - 14

Czas trwania szkolenia – min. 5 godzin

Liczba edycji szkolenia – 1 (planowany termin rok 2024 lub 2025).

Program szkolenia może zostać zmodyfikowany i musi odnosić się do aktualnych zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków obrony przed nimi.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.7.Część 7.: Bezpieczeństwo informacji podczas pracy zdalnej z elementami cyberzagrożeń dla Pracowników Urzędu Gminy Stara Biała

W ramach realizacji części 7. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego dla pracowników Urzędu Gminy Stara Biała w zakresie szacowania ryzyka, w szczególności w kontekście pracy zdalnej, a także jak je prawidłowo przeprowadzić, jakich użyć przepisów krajowych czy też międzynarodowych oraz jakie są wymagane standardy (normy ISO) z zakresu formalnoprawnego oraz dziedziny IT.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Omówienie niezbędnych przepisów celem prawidłowego zrozumienia procesu szacowania ryzyka w kontekście RODO, rozporządzenia Krajowych Ram Interoperacyjności, norm ISO oraz Kodeksu Pracy.
2. Omówienie zjawiska pracy zdalnej w oparciu o aktualnie obowiązujące przepisy prawa w zakresie bezpieczeństwa informacji.
3. Analiza stosowanych aktywów oraz występujących zagrożeń w kontekście standardów ISO.
4. Wskazanie międzynarodowych norm ISO pomocnych w procesie szacowania ryzyka.

5. Wskazanie niezbędnych elementów składających się na szacowanie ryzyka podczas pracy zdalnej.
6. Proces klasyfikacji czynności przetwarzania zidentyfikowanych w jednostce/organizacji w kontekście pracy zdalnej.
7. Omówienie skali podatności, skutku i ryzyka (+ zaznaczenie różnicy pomiędzy szacowaniem jakościowym i ilościowym).
8. Zasady postępowania z ryzykiem.
9. Przygotowanie planu postępowania z ryzykiem.

Wymagana forma przeprowadzenia szkolenia: **szkolenie grupowe w formule on-line.** Zamawiający zapewni salę szkoleniową z komputerem, rzutnikiem.

Liczba osób do przeszkolenia - 31

Czas trwania szkolenia – min. 5 godzin

Liczba edycji szkolenia – 7 (planowany termin rok 2024 lub 2025).

Program szkolenia może zostać zmodyfikowany i musi odnosić się do aktualnych zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków obrony przed nimi.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.8. Część 8.: Szkolenie z zakresu socjotechniki w formule on -line pracowników Urzędu Gminy Stara Biała

W ramach realizacji części 8. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **szkolenie z zakresu socjotechnik**, w szczególności zaprezentowania sposobów postępowania specjalistów posiadających odpowiednie obowiązki w ramach Systemu Zarządzania Bezpieczeństwem Informacji, wdrażanego w Urzędzie w ramach grantu. Szkoleniem zostaną objęci pracownicy Urzędu. W szkoleniu należy położyć nacisk na praktyczne umiejętności oraz testowanie reakcji personelu na różne scenariusze zagrożeń.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. struktura i cele Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie, jego aspekty praktyczne, a także rola i odpowiedzialność poszczególnych pracowników w jego funkcjonowaniu,
2. polityki i procedury związane z bezpieczeństwem informacji obowiązujących w Urzędzie,
3. sposoby poprawy procesów bezpieczeństwa informacji, takie jak ćwiczenia symulacyjne i audyty oraz rola pracowników Urzędu w tych procesach,
4. rozpoznawanie zagrożeń, w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia

z uwzględnieniem oszustwa typu Business E-mail Compromise oraz techniki stosowane w atakach socjotechnicznych, takie jak pretexting, baiting, vishing, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa,

5. wpływ zagrożeń na działalność urzędu, w tym zrozumienie konsekwencji ataków cybernetycznych dla jednostki samorządu terytorialnego, ryzyka utraty danych, naruszenia bezpieczeństwa informacji oraz szkód reputacyjnych,
6. ochrona danych i informacji, w tym podstawowe zasady ochrony danych osobowych i informacji wrażliwych, zgodnie z obowiązującymi przepisami (np. RODO) oraz środki ochrony, takie jak silne hasła, uwierzytelnianie wieloskładnikowe, klucze sprzętowe oraz bezpieczne zarządzanie hasłami,
7. bezpieczeństwo systemów i urządzeń, w tym zasady bezpiecznego korzystania z urządzeń służbowych i systemów informatycznych, unikanie instalacji nieautoryzowanego oprogramowania i regularna aktualizacja systemów operacyjnych i aplikacji,
8. reagowanie na incydenty bezpieczeństwa, w tym procedury zgłaszania incydentów bezpieczeństwa oraz sposoby ich dokumentowania, identyfikowanie potencjalnych incydentów i podejmowanie właściwych działań, współpraca z zespołem IT w celu rozwiązania problemów związanych z bezpieczeństwem oraz zrozumienie, kiedy i jak eskalować problemy do specjalistów,
9. sposoby budowania kultury bezpieczeństwa, metody ciągłego doskonalenie umiejętności, dzielenie się wiedzą, audyty, promocja bezpieczeństwa informacji w codziennej pracy i zachęcanie innych pracowników do przestrzegania najlepszych praktyk, współtworzenie środowiska pracy, w którym bezpieczeństwo jest traktowane jako priorytet.

Wymagana forma przeprowadzenia szkolenia: **szkolenie grupowe w formule on-line.** Zamawiający zapewni salę szkoleniową z komputerem, rzutnikiem.

Liczba osób do przeszkolenia – 31

Czas trwania szkolenia – min. 5 godzin

Liczba edycji szkolenia – 1 (planowany termin rok 2024 lub 2025).

Program szkolenia może zostać zmodyfikowany i musi odnosić się do aktualnych zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków obrony przed nimi.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.9. Część 9.: Szkolenie z zakresu wprowadzenia do bezpieczeństwa systemów Microsoft dla informatyka.

W ramach 9 części zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia z zakresu **wprowadzenia do bezpieczeństwa systemów Microsoft.** Celem szkolenia jest dostarczenie uczestnikowi, który jest jedyną osobą szkoloną, praktycznej wiedzy i umiejętności w zakresie wdrażania, administracji, rozwiązywania problemów oraz wzmacniania bezpieczeństwa systemu Windows Server 2022. Szkolenie ma na celu podniesienie kompetencji uczestnika w zarządzaniu infrastrukturą serwerową opartą na systemie Windows Server, co przełoży się na wzrost efektywności, stabilności oraz bezpieczeństwa operacyjnego w organizacji.

Szkolenie obejmuje następujące bloki tematyczne:

1. Wdrażanie Windows Server 2022

•Przegląd funkcji i możliwości Windows Server 2022.

•Planowanie i konfiguracja wdrożeń serwerów oraz integracja z istniejącą infrastrukturą.

•Instalacja systemu, konfiguracja podstawowych ustawień oraz migracja z wcześniejszych wersji Windows Server.

•Tworzenie, zarządzanie oraz monitorowanie wirtualnych maszyn w oparciu o Hyper-V.

•Tworzenie środowiska redundancji i odzyskiwania po awarii.

2. Rozwiązywanie problemów

•Analiza i diagnostyka problemów na poziomie systemu operacyjnego, usług oraz aplikacji serwerowych.

•Wykorzystanie narzędzi diagnostycznych Windows Server (Event Viewer, Performance Monitor, Windows Admin Center).

•Identyfikacja i rozwiązywanie problemów z siecią, przechowywaniem danych oraz dostępem do zasobów.

•Procedury i najlepsze praktyki rozwiązywania problemów związanych z Active Directory oraz DNS.

•Identyfikacja przyczyn problemów związanych z wydajnością i działania naprawcze.

3. Wzmacnianie bezpieczeństwa

•Przegląd zagrożeń bezpieczeństwa oraz najlepsze praktyki w zakresie ochrony danych na Windows Server 2022.

•Konfiguracja polityk zabezpieczeń, zarządzanie uprawnieniami użytkowników i ról systemowych.

•Wdrażanie zaawansowanych mechanizmów uwierzytelniania, w tym Windows Defender Credential Guard i Secure Boot.

•Konfiguracja mechanizmów ochrony i szyfrowania danych, np. BitLocker, w celu zabezpieczenia przechowywanych informacji.

•Monitorowanie systemu pod kątem zagrożeń i analiza logów związanych z bezpieczeństwem przy użyciu Windows Event Logging i SIEM.

Metodologia i Forma Szkolenia

•Szkolenie obejmuje część teoretyczną oraz praktyczne ćwiczenia z użyciem rzeczywistych systemu Windows Serwer 2022 lub maszyn wirtualnych z tym systemem.•Uczestnik otrzyma dostęp do dedykowanego stanowiska do

ćwiczeń praktycznych.

•Po ukończeniu szkolenia uczestnik może przystąpić do certyfikacyjnego egzaminu, który jest wliczonego w cenę szkolenia, który potwierdzi zdobyte kompetencje.

•Cena Egzaminu jest w cenie szkolenia.

6. Materiały Szkoleniowe

Uczestnik otrzyma pełen zestaw materiałów szkoleniowych w języku polskim, w tym:

•Podręcznik (papierowy lub cyfrowy).

•Dokumentację techniczną.

•Dodatkowe materiały, takie jak prezentacje, instrukcje oraz przykłady konfiguracji.

Wymagania Techniczne

W przypadku szkolenia zdalnego wykonawca zapewni uczestnikowi dostęp do platformy treningowej umożliwiającej pełną symulację środowiska ekosystemu Microsoft Windows Serwer 2022.

Egzamin i Certyfikacja

Po zakończeniu szkolenia uczestnik może przystąpić do certyfikacyjnego egzaminu, który jest wliczonego w cenę szkolenia. Egzamin potwierdzi jego umiejętności i zakończy się wydaniem oficjalnego certyfikatu.

Dodatkowe Wsparcie

W cenę szkolenia wliczony jest 14-dniowe wsparcie ze strony trenera, obejmujące możliwość kontaktu i zadawania pytań związanych z materiałem szkoleniowym, licencjonowaniem oraz administracją systemem Windows Serwer 2022.

Wymagana forma przeprowadzenia szkolenia: szkolenie w formule on-line. Liczba osób do przeszkolenia – 1

Czas trwania szkolenia – Szacowany czas trwania każdego bloku tematycznego to ok. 2 dni robocze, łącznie 6 dni szkoleniowych. Termin realizacji szkolenia: do 30 dni od daty zawarcia umowy. Wykonawca zobowiązany jest do dostarczenia dokumentacji szkoleniowej, raportu z przeprowadzonego szkolenia oraz oceny efektywności szkolenia.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.10. Część 10.: Szkolenie techniczne poświęcone urządzeniom klasy UTM do ochrony styku sieci firmowej z Internetem dla informatyka.

W ramach 10 części zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia technicznego poświęconego urządzeniom UTM do ochrony styku sieci firmowej z Internetem. Celem zamówienia jest przeprowadzenie szkolenia pracowników IT zamawiającego, które umożliwi nabycie wiedzy i praktycznych

umiejętności zarządzania oraz konfigurowania urządzeń sieciowych marki aktualnie użytkowanego w Urzędzie do ochrony styku z internetem.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Podstawowa zarządzania urządzeniem.

•Wprowadzenie do rozwiązań marki aktualnie użytkowanego w Urzędzie do ochrony styku z internetem i ich roli w ochronie sieci.

•Konfigurację i administrację urządzeń marki aktualnie użytkowanego w Urzędzie do ochrony styku z internetem.

•Zarządzanie regułami firewall oraz kontrolą dostępu.

•Konfigurację i zarządzanie VPN (Virtual Private Network).

•Implementację filtrów aplikacji oraz zabezpieczeń na poziomie sieciowym i aplikacyjnym.

•Monitorowanie ruchu sieciowego oraz użycie narzędzi diagnostycznych.

•Zarządzanie licencjami UTM aktualnie użytkowanego w Urzędzie do ochrony styku z internetem:

•Przegląd typów licencji oraz ich aktywacji i przedłużenia.

•Praktyczne zarządzanie licencjami oraz ich monitorowanie.

2. Zaawansowana konfiguracja IPS.

•Technologia ASQ i fazy analizy pakietu w szczegółach,

•Wykorzystanie profili IPS,

•Zmiana domyślnych profili dla ruchu wchodzącego i wychodzącego z sieci,

•Zapisywanie i analiza pakietów dzięki sygnaturom kontekstowym,

•Łączenie profili IPS z regułami filteringu.

3. Zaawansowana konfiguracja sieci.

•Interfejsy typu Dialup,

•Interfejsy typu VLAN.

4. Zaawansowana konfiguracja routingu.

•Routing by interface,

•Policy routing,

•Load balancing.

5. Zaawansowana translacja adresów.

6. Zaawansowana konfiguracja firewalla.

7. Kształtowanie pasma (QoS).

•Omówienie mechanizmu Quality of Service (QoS),

•Konfiguracja kolejek QoS z wykorzystaniem algorytmu PRIQ,

•Konfiguracja kolejek QoS z wykorzystaniem algorytmu CBQ,

•Monitorowanie ruchu z wykorzystaniem kolejek QoS typu MONITOR,

•Integracja kolejek QoS z firewallem.

8. Infrastruktura Klucza Publicznego.

•Wprowadzenie to tematyki Public Key Infrastructure (PKI).

•Tworzenie wewnętrznego urzędu certyfikacji,

•Integracja PKI z innymi usługami w urządzeniu,

•Integracja urządzenia z zewnętrznym urzędem certyfikacji.

9. Technologia VPN.

•IPSec VPN.

•Kanały VPN typu site-to-site z wykorzystaniem protokołu IPSec (PKI),

•Kanały VPN typu client-to-site z wykorzystaniem protokołu IPSec (PKI),

•Translacja adresów w tunelach IPSec,

•Zaawansowane opcje IPSec VPN.

•SSL VPN.

•Konfiguracja SSL VPN w trybie Portal,

•Konfiguracja SSL VPN w trybie Tunel.

10. Zaawansowane opcje Proxy - SSL Proxy.

•Wprowadzenie do SSL Proxy,

•Konfiguracja certyfikatów dla SSL Proxy

11. Zarządzanie urządzeniem z wykorzystaniem CLI.

•Rozwiązywanie problemów konfiguracyjnych,

•Tworzenie i analiza technical repor.

Metodologia i Forma Szkolenia

•Szkolenie obejmuje część teoretyczną oraz praktyczne ćwiczenia z użyciem rzeczywistych urządzeń lub symulatorów urządzeń marki aktualnie użytkowanego w Urzędzie do ochotny styku z internetem.

•Szkolenie trwa minimum 3 dni (około 24h łącznie), w formie zdalnej, zgodnie z ustaleniami z zamawiającym.

•Uczestnik otrzyma dostęp do dedykowanego stanowiska do ćwiczeń praktycznych.

•Po ukończeniu szkolenia uczestnik może przystąpić do certyfikacyjnego egzaminu, który jest wliczonego w cenę szkolenia, który potwierdzi zdobyte kompetencje.

•Cena Egzaminu jest w cenie szkolenia.

Materiały Szkoleniowe

Uczestnik otrzyma pełen zestaw materiałów szkoleniowych w języku polskim, w tym:

•Podręcznik (papierowy lub cyfrowy).

•Dokumentację techniczną dotyczącą urządzeń aktualnie użytkowanego w Urzędzie do ochrony styku z internetem i zarządzania licencjami UTM.

•Dodatkowe materiały, takie jak prezentacje, instrukcje oraz przykłady konfiguracji.

Wymagania Techniczne

W przypadku szkolenia zdalnego wykonawca zapewni uczestnikowi dostęp do platformy treningowej umożliwiającej pełną symulację środowiska aktualnie użytkowanego urządzania do ochrony sieci.

Egzamin i Certyfikacja

Po zakończeniu szkolenia uczestnik może przystąpić do certyfikacyjnego egzaminu., wliczonego w cenę szkolenia. Egzamin potwierdzi jego umiejętności i zakończy się wydaniem oficjalnego certyfikatu.

Dodatkowe Wsparcie

W cenę szkolenia wliczone jest 14-dniowe wsparcie ze strony trenera, obejmujące możliwość kontaktu i zadawania pytań związanych z materiałem szkoleniowym, licencjonowaniem UTM oraz administracją urządzeniami.

10. Harmonogram i Miejsce Realizacji

•Szkolenie powinno być zrealizowane do końca roku 2024 roku.

•Termin realizacji szkolenia zostanie ustalony w ciągu 14 dni od momentu podpisania umowy.

•Miejsce realizacji: zdalne (do uzgodnienia z zamawiającym).

Wymagania Końcowe

Po zakończeniu szkolenia wykonawca dostarczy zamawiającemu materiały informacje o zakresie tematycznym, obecności uczestnika oraz wynikach egzaminu certyfikacyjnego.

•pakiet materiałów szkoleniowych,

•zaświadczenie dla uczestnika który ukończył szkolenie.

•opcjonalnie egzamin,

•certyfikat dla osoby, która zda egzamin,

•14-to dniowy kontakt z trenerem po szkoleniu.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

5.11. Część 11.: Audytor wiodący systemów zarządzania bezpieczeństwem informacji zgodnie z ISO 27001

W ramach części 11 zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego dla jednego pracownika Urzędu Gminy Stara Biała. Cel szkolenia: Zrozumienie wymagań i wytycznych norm PN-EN

ISO/IEC 27001:2023, PN-EN ISO/IEC 27002:2023, PN-ISO 27006:2016-12 i PN-EN ISO 19011:2018-08. Zdobycie wiedzy dotyczącej zasad audytowania w obszarze bezpieczeństwa informacji. Szkolenie powinno zakończyć się uzyskaniem przez pracownika certyfikatu ukończenia szkolenia z akredytacją PCA.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Zapoznanie z wymaganiami normy ISO/IEC 27001:2022 (norma ta jest tożsama z PN-EN ISO/IEC 27001:2023);
2. Wzajemne relacje między PN-EN ISO/IEC 27001:2023, PN-EN ISO/IEC 27002:2023, PN- ISO 27006:2016-12 i PN-EN ISO 19011:2018-08;
3. Audyt trzeciej strony – wybrane wymagania PN-EN ISO/ IEC 17021-1;
4. Podejście procesowe do ochrony informacji i bezpieczeństwa systemów informatycznych przedsiębiorstw;
5. Ustanowienie, rozwój i utrzymanie systemów informacyjnych;
6. Podstawowe pojęcia dotyczące urządzeń, systemów i sieci informacyjnych - analiza i ocena ryzyka;
7. Krytyczne sytuacje audytu systemu zarządzania bezpieczeństwem informacji;
8. Podstawy audytowania – rodzaje audytów;
9. Metody i techniki audytowania – planowanie (plan audytu, pytania audytowe / checklista) i przeprowadzanie audytu;
10. Sprawozdawczość z audytu, działania wynikające z audytu (korygujące, korekcyjne, doskonalące oraz zapobiegawcze), przygotowanie raportu z audytu bezpieczeństwa informacji;
11. Ustalenia audytowe, ocena wyników/ zgodności /niezgodności oraz zarządzanie niezgodnościami;
12. Polityka bezpieczeństwa, organizacja bezpieczeństwa informacji;
13. Zarządzanie aktywami;
14. Bezpieczeństwo fizyczne i środowiskowe;
15. Zarządzanie komunikacją i operacjami, kontrola dostępu;
16. Zarządzanie incydentami w bezpieczeństwie informacji;

domyślnej ochrony danych, a także weryfikacja takiej dokumentacji.

Wymagana forma przeprowadzenia szkolenia: szkolenie w formule on-line. Zamawiający zapewni salę szkoleniową z komputerem, rzutnikiem.

Liczba osób do przeszkolenia – 1

Czas trwania szkolenia – 5 dni szkoleniowych

Liczba edycji szkolenia – 1 (planowany termin rok 2024 lub 2025).

Z przeprowadzonego szkolenia Wykonawca musi przedstawić potwierdzenie realizacji szkolenia.

Szkolenie musi być zakończone oceną szkolenia, jego przydatności, zakresu przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

6. Harmonogram realizacji zamówienia

Zamówienie (wszystkie części) musi zostać zrealizowane nie później niż do 5 maja 2026 r.

UWAGA! Dokładne daty rozpoczęcia realizacji poszczególnych szkoleń (części 1. – 11.) zostaną uzgodnione pomiędzy Zamawiającym i Wykonawcą.

7. Warunki udziału w postępowaniu

O udzielenie poszczególnych części zamówienia mogą ubiegać się Wykonawcy nie podlegający wykluczeniu i spełniający warunki udziału w postępowaniu, dotyczące **zdolności technicznej lub zawodowej**, którzy:

dla części 1. – 8.:

1. mają co najmniej 3-letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń,
2. zrealizowali w okresie ostatnich trzech lat co najmniej 3 zamówienia obejmujące wykonanie co najmniej 10 szkoleń z zakresu cyberbezpieczeństwa w jednostkach sektora finansów publicznych,
3. dysponują lub będą dysponować co najmniej 2 trenerami, którzy będą uczestniczyć w realizacji zamówienia, z których każdy:
   - ma wykształcenie wyższe,
   - posiada certyfikat audytora wiodącego ISO/IEC 27001 w wersji 2007 lub nowszej lub inny certyfikat wymieniony w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999),
   - przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 50 godzin (zegarowych) szkoleń na temat cyberbezpieczeństwa.

Dla części 9.:

1. Mają co najmniej 5-letnie doświadczenie w przeprowadzaniu autoryzowanych szkoleń Microsoft oraz posiadają status oficjalnego partnera szkoleniowego Microsoft

2. Zrealizowali w okresie ostatnich trzech lat co najmniej 3 zamówienia obejmujące wykonanie szkoleń z zakresu Windows Serwer.

3. Dysponują lub będą dysponować co najmniej 2 trenerami, którzy będą uczestniczyć w realizacji zamówienia, z których każdy:

- ma wykształcenie wyższe, posiada tytuł certyfikowanego trenera Microsoft Certified Trainer (MCT)
- Posiadanie odpowiednich certyfikatów potwierdzających kompetencje szkoleniowców w zakresie Microsoft Windows Server np. Microsoft Certified: Windows Server Hybrid Administrator Associate:

Exams: AZ-800: Administering Windows Server Hybrid Core Infrastructure oraz AZ-801: Configuring Windows Server Hybrid Advanced Services.

Microsoft Certified Solutions Associate (MCSA):

Exams: Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022.

Microsoft Certified Solutions Expert (MCSE):

4. Przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 50 godzin (zegarowych) szkoleń na temat Windows Serwer.

5. Doświadczenie w przeprowadzaniu szkoleń z obszaru administracji Windows Server – min. 5 Lat.

6. Dostarczenie materiałów szkoleniowych oraz zapewnienie dostępu do środowiska testowego w tym oficjalnych laboratoriów Microsoft oraz dostęp do nich przez minimum 5 miesięcy od daty zakończenia szkolenia.

7. Wykonawca posiada minimum 5 lat kompetencje autoryzowanego centrum egzaminacyjnego, umożliwiającego przeprowadzenie egzaminów w zakresie technologii Microsoft.

dla części 10.:

Wykonawca musi posiadać autoryzację producenta aktualnie użytkowanego w Urzędzie do ochrony styku z internetem do prowadzenia certyfikowanych szkoleń CSNA. Szkolenie musi być prowadzone przez certyfikowanego instruktora z aktualną wiedzą na temat zarządzania licencjami oraz praktycznej administracji urządzeniami UTM aktualnie użytkowanego w Urzędzie do ochrony styku z internetem.

1. Mają co najmniej 2-letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń z zakresu administracji urządzeniami klasy UTM.

2. Zrealizowali w okresie ostatnich trzech lat co najmniej 3 zamówienia obejmujące wykonanie szkoleń z zakresu zarządzania urządzeniami marki aktualnie użytkowanego w Urzędzie do ochrony styku z internetem

3. Dysponują lub będą dysponować co najmniej 2 trenerami, którzy będą uczestniczyć w realizacji zamówienia, z których każdy:

- ma wykształcenie wyższe,
- Posiadanie odpowiednich certyfikatów potwierdzających kompetencje szkoleniowców w zakresie zarządzania urządzaniami marki aktualnie użytkowanego w Urzędzie do ochrony styku z internetem.

4. Przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 20 godzin (zegarowych) szkoleń na temat Windows Serwer.

5. Doświadczenie w przeprowadzaniu szkoleń z obszaru administracji Windows Server – min. 5 lat.

6. Dostarczenie materiałów szkoleniowych oraz zapewnienie dostępu do środowiska testowego.

dla części 11.:

- Wykonawca musi dysponować przynajmniej jedną osoba posiadającą Certyfikat systemów zarządzania jakością wg PN-EN ISO/IEC 27001:2017, ISO/IEC 27001:2022, PN-EN ISO 22301:2020 z ramienia jednostki

certyfikującej systemy;

- Min. 3 letnie doświadczenie w prowadzeniu szkoleń zarówno w obszarze wymagań prawnych jak i systemowych związanych z bezpieczeństwem informacji;
- Min. 3 letnie doświadczenie jako audytor jednostek certyfikujących.

Na potwierdzenie spełnienia ww. warunków Wykonawca zobowiązany jest przedstawić:

- **wykaz usług** zrealizowanych w okresie ostatnich trzech lat przed upływem terminu składania ofert – wzór wykazu stanowi **załącznik nr 2** do niniejszego zapytania ofertowego.
- **wykaz osób** przeznaczonych do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za przeprowadzenie szkoleń, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień i doświadczenia niezbędnego do wykonania zamówienia, a także kopiami dokumentów potwierdzającymi posiadane doświadczenie i certyfikaty – wzór wykazu stanowi **załącznik nr 3** do niniejszego zapytania ofertowego.

8. Wykluczenie z udziału w postępowaniu

O udzielenie zamówienia nie może ubiegać się Wykonawca w stosunku do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2023 r. poz. 1497 z późn. zm.);

Zamawiający wykluczy z postępowania wykonawcę, który jest powiązany z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

1. uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej,
2. posiadaniu co najmniej 10% udziałów lub akcji,
3. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
4. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

9. Sposób przygotowania oferty

1. Ofertę należy sporządzić na formularzu ofertowym stanowiącym **załącznik nr 1.** do niniejszego zapytania

ofertowego.

2. Do oferty musi zostać załączony wykaz usług stanowiący **załącznik nr 2** do niniejszego zapytania ofertowego oraz wykaz osób przeznaczonych do realizacji zamówienia stanowiący **załącznik nr 3.**
3. Cena oferty musi być ceną ryczałtową, obejmować dowolną liczbę części zamówienia w całości i być podana w złotych polskich. Cena musi być rozbita na kwoty cząstkowe stanowiące wynagrodzenie za realizację poszczególnych części zamówienia i edycji szkoleń.
4. Oferta winna być podpisana przez osobę/y upoważnione do reprezentowania Wykonawcy.
5. **Ofertę należy podpisać podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisem zaufanym.**
6. Wykonawca ma prawo złożyć tylko 1 ofertę w zakresie 1 części. Złożenie przez Wykonawcę więcej niż 1 oferty w zakresie 1 części, skutkuje odrzuceniem wszystkich ofert złożonych przez tego Wykonawcę.
7. Wszelkie koszty przygotowania oferty ponosi Wykonawca.
8. Nie przewiduje się zwrotu kosztów udziału w postępowaniu.
9. Termin związania ofertą wynosi 30 dni.
10. Wykonawca informuje Zamawiającego o informacjach zawartych w ofercie stanowiących tajemnicę przedsiębiorstwa.

10. Wymagane dokumenty

Wraz z ofertą Wykonawca jest zobowiązany złożyć dokumenty potwierdzające należytą realizację zamówień wymienionych w wykazie usług oraz certyfikaty potwierdzające posiadanie przez audytorów uprawnień wymienione w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

11. Miejsce i termin składania ofert:

1. Ofertę wraz z załącznikami należy złożyć za pośrednictwem portalu Baza Konkurencyjności – https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl **w terminie do dnia 03.12.2024 r. do godziny 10:00.**
2. O terminowym złożeniu oferty decyduje data złożenia oferty za pośrednictwem portalu Baza Konkurencyjności.
3. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
4. Ofertę wraz z załącznikami składa się, pod rygorem nieważności, w postaci elektronicznej **podpisanej**

kwalifikowanym podpisem elektronicznym lub **podpisem zaufanym** przez osobę/y upoważnioną/e do reprezentowania wykonawcy. Brak podpisu/ów w wymieniony sposób będzie skutkował odrzuceniem oferty.

5. Oferta winna być sporządzona w języku polskim pod rygorem nieważności. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem przysięgłym na język polski.
6. **Zamawiający nie dopuszcza innej formy i sposobu składania ofert niż za pośrednictwem portalu Baza Konkurencyjności**. Niespełnienie tego wymogu oznacza niezgodność oferty z Zapytaniem. Oferty złożone w inny sposób zostaną odrzucone przez Zamawiającego.

12. Kryteria wyboru oferty

1. Przy wyborze oferty Zamawiający będzie się kierował następującym kryterium:

   cena brutto – 100%

   Wybrana zostanie oferta z największą ilością punktów spośród ofert nieodrzuconych, obliczoną zgodnie z poniżej określonym wzorem:

$$\frac{Najniższa\ cena\ spośród\ ofert\ nieodrzuconych}{Cena\ oferty\ badanej} \times 100$$

2. W sytuacji gdy cena najkorzystniejszej oferty będzie znacząco przewyższała środki zabezpieczone przez Zamawiającego w budżecie, Zamawiający zastrzega sobie możliwość przeprowadzenia dodatkowych negocjacji z Wykonawcą, który złoży najkorzystniejszą ofertę.
3. W przypadku gdy wybrany Wykonawca odstąpi od podpisania umowy z Zamawiającym, możliwe jest podpisanie przez Zamawiającego umowy z kolejnym Wykonawcą, który w postępowaniu uzyskał kolejną najwyższą liczbę punktów.
4. Zamawiający może w toku badania i oceny ofert żądać od Oferentów dodatkowych wyjaśnień dotyczących treści złożonych ofert.
5. Zamawiający wyjaśni i poprawi w formularzu ofertowym:
   - oczywiste omyłki pisarskie,
   - oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   - inne omyłki polegające na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty.
6. Poprawienie przez Zamawiającego oczywistych omyłek pisarskich oraz rachunkowych i konsekwencji rachunkowych dokonanych poprawek nie wymaga uzyskania zgody wykonawcy. Wykonawca może nie wyrazić zgody na poprawienie przez zamawiającego innych omyłek polegających na niezgodności oferty z

opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty. Brak zgody Wykonawca musi wnieść na piśmie w wyznaczonym przez Zamawiającego terminie.

7. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez dokonania wyboru żadnej z ofert, bez podania przyczyny, na każdym etapie prowadzonego postępowania. Z tytułu unieważnienia postępowania, Wykonawcy nie przysługuje żadne roszczenie wobec Zamawiającego.

13. Kontakt z Zamawiającym

1. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji między Zamawiającym a Wykonawcą oraz przekazywanie dokumentów i oświadczeń odbywa się pisemnie za pomocą portalu Bazy Konkurencyjności
2. Po stronie Zamawiającego osobą do kontaktów w sprawie zamówienia jest:

   Aleksandra Kozłowska
   Inspektor ds. inwestycji i funduszy pomocowych Referat Inwestycji i rozwoju
   tel.: +48 24 366 87 29
   e-mail: a.kozlowska@starabiala.pl

3. W tytule wiadomości należy wskazać numer zapytania ofertowego – Znak IR.IFS.041.30.1.2023

14. Wyjaśnienia oraz uzupełnienia do oferty

1. W toku badania ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonej oferty, treści oświadczeń, dokumentów, pełnomocnictw i ich uzupełnienia
2. Jeżeli zaoferowana cena będzie rażąco niska w stosunku do przedmiotu zamówienia lub będzie budziła wątpliwości co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, Zamawiający zwróci się do wykonawcy o udzielenie wyjaśnień, w tym złożenie dowodów dotyczących wyliczenia ceny. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu będzie spoczywać na Wykonawcy.
3. Zamawiający odrzuci ofertę Wykonawcy, który nie udzieli wyjaśnień, o których mowa powyżej lub jeżeli dokonana ocena tych wyjaśnień wraz ze złożonymi dowodami potwierdzi, że zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.

15. Klauzula informacyjna RODO

Realizując obowiązek wynikający z art. 13, 14 i 15 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 – zwanego RODO uprzejmie informuję, że:

1) Administratorem Państwa danych osobowych jest Wójt Gminy Stara Biała, ul. Jana Kazimierza 1, 09-411 Biała.

2) Inspektorem Ochrony Danych w Urzędzie Gminy Stara Biała jest Pani Magdalena Łabędzka, adres e-mail: iod@starabiala.pl

3) W Urzędzie Gminy Stara Biała Państwa dane osobowe przetwarza się na podstawie obowiązujących przepisów prawa, zawartych umów oraz na podstawie udzielonej zgody w celu:

1) wypełnienia ciążących na Administratorze obowiązków prawnych;

2) realizacji umów, których stroną jest Gmina bądź Urząd;

3) w pozostałych przypadkach Państwa dane osobowe przetwarzane są wyłącznie na podstawie wcześniej, dobrowolnie udzielonej zgody w zakresie i celu określonym w treści zgody. W pewnych sytuacjach niepodanie danych w zakresie wymaganym przez Administratora może skutkować niemożnością realizacji usługi.

Państwa dane osobowe mogą zostać udostępnione:

1) organom władzy publicznej oraz podmiotom wykonującym zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa;

2) innym podmiotom, które na podstawie stosownych umów przetwarzają dane osobowe których Administratorem jest Wójt Gminy Stara Biała.

Państwa dane osobowe mogą być przetwarzane w sposób zautomatyzowany, natomiast nie będą one profilowane oraz przekazywane do państw trzecich.

Okres przechowywania danych osobowych określa rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, chyba, że przepisy ustaw stanowią inaczej, z wyłączeniem:

1) nagrań rozmów telefonicznych i zapisów formularzy kontaktowych obsługiwanych przez Urząd Gminy Stara Biała – do chwili całkowitego zapisu dysku twardego na którym zapisywane są nagrania;

2) nagrań z monitoringu wizyjnego budynku – do chwili całkowitego zapisu dysku twardego na którym zapisywane są nagrania.

Przysługuje Państwu prawo dostępu do swoich danych osobowych, ich sprostowania, usunięcia, przenoszenia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania danych osobowych, a także prawo do cofnięcia wcześniej udzielonej zgody.

Jeżeli uznacie Państwo, że dane osobowe, których Administratorem jest Wójt Gminy Stara Biała są

przetwarzane niezgodnie z prawem możecie Państwo wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych.

Załączniki:

1. Formularz oferty
2. Oświadczenie o braku powiązań z Zamawiającym i braku podstaw do wykluczenia
3. Wykaz usług
4. Wykaz osób przeznaczonych do realizacji zamówienia
5. Projektowane postanowienia umowy
6. Klauzula informacyjna RERC

Sławomir Stanisław Wawrzyński; Wójt ;Gmina Stara Biała

Elektronicznie podpisany przez Sławomir Stanisław Wawrzyński; Wójt ;Gmina Stara Biała
Data: 2024.11.25 13:12:37 +01'00'