



Cyberbezpieczny Samorząd



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

nr umowy:/WO/25

zawarta w dniu r. w Krobi (zwana dalej „Umową”)

pomiędzy:

Gminą Krobia, z siedzibą w Krobi 63-840 ul. Rynek 1,

reprezentowaną przez:

Łukasza Kubiaka - Burmistrza Krobi,

przy kontrasygnacie Skarbnika Gminy Damiana Walczaka

zwaną dalej „Zamawiającym”,

a

.....
.....
.....

zwaną/ym dalej „Wykonawcą”,

łącznie zwanymi „Stronami”,

o następującej treści:

§ 1

Przedmiot umowy

1. Zamawiający powierza do wykonania, a Wykonawca zobowiązuje się do realizacji zadania pod nazwą: **„Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Gminie Krobia w ramach konkursu grantowego ”Cyberbezpieczna Gmina Krobia”**.

2. Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC).

3. Szczegółowy przedmiot zamówienia znajduje się w załączniku nr 1 do Umowy.

§ 2

Termin realizacji

1. Wykonawca zobowiązuje się wykonać przedmiot umowy **w terminie:**

Etap 1 – Do 60 dni od podpisania umowy

Etap 2- Do 90 dni od podpisania umowy

Etap 3 - Po zakończeniu etapu 2 nie później niż do 31 grudnia 2025

Etap 4- - Po zakończeniu etapu 2 nie później niż do 31 grudnia 2025

Etap 5 – Do 60 dni od zakończenia etapu 2

Etap 6- Nie wcześniej niż 1 stycznia 2026 nie później niż 11 miesięcy od podpisania umowy

2. Termin zakończenia zadania, o którym mowa w ust. 1 uważa się za zachowany, jeśli w tym terminie Wykonawca dokonała pisemnego zgłoszenia Zamawiającemu zakończenia zadania.

§ 3

Wynagrodzenie

1. Za wykonanie przedmiotu umowy określonego w § 1 niniejszej umowy, Strony ustalają wynagrodzenie ryczałtowe w wysokości:

..... zł **netto** (słownie: 00/100) powiększone o podatek VAT, co daje kwotę zł brutto (słownie: 00/100).

2. Płatność za wykonanie przedmiotu Umowy, nastąpi w ciągu **do 14 dni** od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury.

3. Podstawą wystawienia faktury będzie podpisany ze strony Zamawiającego protokół zdawczo-odbiorczy częściowy lub końcowy podpisany przez strony umowy.

4. Zamawiający dopuszcza fakturowanie częściowe podczas realizacji zamówienia

5. Wynagrodzenie ryczałtowe, o którym mowa w ust. 1 obejmuje wszystkie koszty związane z realizacją przedmiotu umowy, w tym ryzyko Wykonawcy z tytułu oszacowania wszelkich kosztów związanych z realizacją przedmiotu umowy, a także oddziaływania innych czynników mających lub mogących mieć wpływ na koszty.

Niedoszacowanie, pominięcie oraz brak rozpoznania zakresu przedmiotu umowy nie może być podstawą do żądania zmiany wynagrodzenia ryczałtowego określonego w ust. 1 niniejszego paragrafu.

6. Zamiast faktury w formie papierowej lub elektronicznej wystawionej na Gminę Krobia Wykonawca ma możliwość (ale nie jest obowiązany) wystawiania i wysyłania ustrukturyzowanych faktur elektronicznych do Gminy Krobia za pośrednictwem platformy elektronicznego fakturowania <https://brokerpefexpert.efaktura.gov.pl> na adres PEF: NIP 6961749038 – w przypadku wystawiania faktur elektronicznych na wskazany adres PEF Nabywcą/Odbiorcą towaru/usługi jest **Gmina Krobia, ul. Rynek 1, 63-840 Krobia, NIP: 6961749038.**

7. Zamawiający jest obowiązany do odbierania od Wykonawcy ustrukturyzowanych faktur elektronicznych przesłanych za pośrednictwem platformy na adres PEF wskazany przez Zamawiającego. Przepisu art. 106n ust. 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług nie stosuje się.

8. Zgodnie z art. 4 ust. 4 ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz.U. z 2020 r. poz. 1666 ze zm.), Zamawiający i Wykonawca mogą wysyłać i odbierać inne ustrukturyzowane dokumenty elektroniczne za pośrednictwem platformy, jeżeli druga strona wyrazi na to zgodę.

§ 4

Odbiór przedmiotu zamówienia

1. Etap 1 - W celu potwierdzenia Zamawiający oczekuje raportu z audytu dostarczonego do Zamawiającego w formie papierowej lub elektronicznej opatrzonej podpisem kwalifikowanym .Opracowanie raportu zawierającego wykryte podatności podzielone i przypisane, według wielkości zagrożenia. Raport powinien zawierać opis rekomendowanych działań zapobiegawczych zmierzających do wyeliminowania i/ lub ograniczenia podatności oraz wszelkich rozwiązań podnoszących poziom ochrony sieci.

2. Etap. 2 - Na potwierdzenie realizacji wykonawca dostarczy :

- a) Dokumentację dotyczącą opracowanego/ zaktualizowanego Systemu Zarządzania Bezpieczeństwem Informacji zgodną z opisem przedmiotu zamówienia
- b) Raport przedstawiający ryzyko występujące w organizacji z ewentualnymi zaleceniami
- c) raport z rekomendacjami i procedury zapewniające plan ciągłości działania w oparciu o normę 22301.

3. Etap 3 - Na potwierdzenie realizacji zadania wykonawca dostarczy :

Dokumentację wszystkich szkoleń, na którą składają się:

- a) Lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).
- b) Lista zaświadczeń o ukończeniu szkolenia.
- c) Kserokopie zaświadczeń o ukończeniu szkolenia
- d) Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie. Zamawiający dopuszcza dokument elektroniczny podpisany cyfrowo.

4. Etap 4 - Na potwierdzenie realizacji zadania wykonawca dostarczy :

Dokumentację wszystkich szkoleń, na którą składają się:

- a) Lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).
- b) Lista zaświadczeń o ukończeniu szkolenia.
- c) Kserokopie zaświadczeń o ukończeniu szkolenia
- d) Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie. Zamawiający dopuszcza dokument elektroniczny podpisany cyfrowo.

5. Etap 5 - Po zakończeniu audytu Wykonawca przygotowuje i przekaże w formie papierowej lub elektronicznej opatrzonej podpisem kwalifikowanym raport z przeprowadzonego audytu i nanieś dane do ankiety wskazanej w załączniku nr 6 do regulaminu konkursu.

6. Etap 6 - Na potwierdzenie realizacji zadania wykonawca dostarczy :

Dokumentację wszystkich szkoleń, na którą składają się:

- a) Lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).
- b) Lista zaświadczeń o ukończeniu szkolenia.
- c) Kserokopie zaświadczeń o ukończeniu szkolenia
- d) Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie. Zamawiający dopuszcza dokument elektroniczny podpisany cyfrowo.

7. Zamawiający dokona odbioru przedmiotu zgodnie z opisem przedmiotu zamówienia.

8. Zamawiający dopuszcza odbiór częściowy zamówienia zgodnie z opisanymi etapami.

9. Podstawą do określenia terminu zakończenia realizacji danego etapu będzie podpisany ze strony Zamawiającego protokół zdawczo-odbiorczy częściowy podpisany przez strony umowy.

10. Na potwierdzenie realizacji całego zadania wykonawca przygotowuje w uzgodnieniu z zamawiającym protokół odbioru końcowego.

11. Wykonawca ponosi wszystkie koszty związane z dostarczeniem przedmiotu umowy do Zamawiającego oraz odpowiada za przedmiot umowy (ryzyko utraty, uszkodzenia itd.) do czasu jego odbioru przez Zamawiającego

§ 5

Podwykonawcy

1. Wykonawca może zrealizować usługi wskazane w ofercie korzystając z pomocy podwykonawców i dalszych podwykonawców na zasadach określonych w Umowie oraz w ustawie Pzp.

2. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.

3. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.

4. Umowa o podwykonawstwo nie może zawierać postanowień kształtujących prawa i obowiązki podwykonawcy w zakresie kar umownych oraz postanowień dotyczących warunków wypłaty wynagrodzenia, w sposób dla niego mniej korzystny niż prawa i obowiązki wykonawcy, ukształtowane postanowieniami umowy zawartej między zamawiającym a wykonawcą.

§ 6

Gwarancja i rękojmia

1. Wykonawca udziela Zamawiającemu rękojmi na Przedmiot Umowy na okres 2 lat.

2. Bieg okresu rękojmi rozpoczyna się w dniu podpisania protokołu zdawczo – odbiorczego, o którym mowa w § 4 Umowy.

3. Zamawiający może dochodzić roszczeń z tytułu rękojmi także po okresie określonym w ust. 1 powyżej, jeżeli zgłosił wadę przed upływem tego okresu.
4. Jeżeli Wykonawca nie usunie wad w terminie określonym przez Zamawiającego, to Zamawiający może zlecić usunięcie ich stronie trzeciej na koszt Wykonawcy, bez zgody sądu. Zamawiający powiadomi pisemnie Wykonawcę o skorzystaniu z powyższego uprawnienia. W przypadku zastępczego usuwania wad podstawą do obciążenia Wykonawcy przez Zamawiającego będzie faktura wystawiona Zamawiającemu przez podmiot usuwający wady. Obciążenie Wykonawcy nastąpi poprzez wystawienie przez Zamawiającego faktury. Wykonawca zapłaci na rzecz Zamawiającego należność wynikającą z faktury w terminie 14 (słownie: czternaście) dni od daty jej otrzymania.

§ 7

Kary umowne

1. Wynagrodzenie umowne dla ustalenia kar umownych – jest to wynagrodzenie ryczałtowe (brutto) określone w niniejszej umowie.
2. Wykonawca zapłaci Zamawiającemu kary umowne w następujących przypadkach:
 - 1) w przypadku odstąpienia przez Zamawiającego lub Wykonawcę od niniejszej Umowy lub rozwiązania Umowy z powodu okoliczności leżących po stronie Wykonawcy, Zamawiającemu przysługuje prawo żądania kary umownej w wysokości 3% wynagrodzenia umownego,
 - 2) w przypadku odstąpienia przez Wykonawcę lub Zamawiającego od niniejszej Umowy lub rozwiązania Umowy z powodu okoliczności leżących po stronie Zamawiającego, Wykonawcy przysługuje prawo żądania kary umownej w wysokości 2% wynagrodzenia umownego,
 - 3) za zwłokę w zakończeniu wykonania przedmiotu umowy – w wysokości 0,1 % wynagrodzenia umownego za każdy dzień zwłoki,
 - 4) za zwłokę w usuwaniu wad stwierdzonych w okresie rękojmi lub gwarancji w wysokości 0,1 % wartości wynagrodzenia umownego brutto Wykonawcy, za każdy rozpoczęty dzień zwłoki w stosunku do terminów przyjętych w Umowie lub uzgodnionych przez strony.
3. Strony zastrzegają sobie prawo do odszkodowania na zasadach ogólnych, o ile wartość faktycznie poniesionych szkód przekroczy wysokość kar umownych.
4. Łączna maksymalna wysokość kar umownych, których mogą dochodzić strony nie może przekraczać 50% wynagrodzenia ryczałtowego (brutto).

§ 8

Zmiana treści umowy

1. Kierując się zapisami art. 455 ust. 1 pkt 1 ustawy Prawo zamówień publicznych, Zamawiający dopuszcza dokonanie zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy w następujących przypadkach:
 - a) zmiany rozwiązań ze względu na postęp techniczny lub technologiczny (np. wycofanie z obrotu urządzeń lub podzespołów), zmiana nie może spowodować podwyższenia ceny oraz obniżenia parametrów technicznych, jakościowych i innych wynikających z oferty (opisu przedmiotu zamówienia / opisu oferowanego towaru), na podstawie której był dokonany wybór Wykonawcy,
 - b) gdy nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie

mającym wpływ na realizację umowy, w tym: zmiana stawki podatku od towarów i usług na asortyment stanowiący przedmiot umowy oraz podatku akcyzowego – w takim przypadku obniżenie lub podwyższenie wynagrodzenia jest możliwe w wysokości odpowiadającej zmianie podatku od towarów i usług oraz podatku akcyzowego,

- c) zmiany terminu realizacji zamówienia z powodu działania siły wyższej, za które uważa się zdarzenia o charakterze nadzwyczajnym, występujące po zawarciu umowy, a których Strony nie były w stanie przewidzieć w momencie jej zawarcia i których zaistnienie lub skutki uniemożliwiają wykonanie przedmiotu umowy w terminie, przy czym ewentualne przedłużenie terminu realizacji zamówienia nastąpi o liczbę dni, odpowiadającą okresowi występowania siły wyższej - podstawą dokonania zmian, o których mowa wyżej będzie wystąpienie opisanych okoliczności uzasadniających wstrzymanie dostaw, z określeniem okresu wpływającego na zmianę terminu i sporządzenie protokołu konieczności – zatwierdzonego przez Zamawiającego
- d) zaistnienie okoliczności leżących po stronie Zamawiającego, w szczególności spowodowanych sytuacją finansową, zdolnościami płatniczymi lub warunkami organizacyjnymi; zmianie może ulec termin realizacji zamówienia, zmiana zostanie wprowadzona stosownie do pisma Zamawiającego określającego te okoliczności.

- 2. Wykonawca wnioskujący o zmianę umowy, przedkłada Zamawiającemu pisemne uzasadnienie konieczności wprowadzenia zmian do umowy wraz z niezbędnymi dowodami.
- 3. Wszelkie zmiany i uzupełnienia treści niniejszej umowy wymagają aneksu sporządzonego z zachowaniem formy pisemnej pod rygorem nieważności.
- 4. Zmiany mogą być dokonane tylko, jeżeli jest to niezbędne dla prawidłowego wykonania przedmiotu umowy.
- 5. Zgodnie z art. 439 ustawy Prawo zamówień publicznych, wysokość wynagrodzenia należnego Wykonawcy może podlegać waloryzacji.
- 6. Zamawiający przewiduje możliwość zmiany wysokości wynagrodzenia na następujących zasadach:

- 1) podstawą ustalania zmian będą Wskaźniki cen producentów usług związanych z obsługą działalności gospodarczej ogłaszane w komunikacie Prezesa Głównego Urzędu Statystycznego (pozycja: Działalność związana z oprogramowaniem i doradztwem w zakresie informatyki oraz działalność powiązana),
- 2) przez zmianę rozumie się wzrost jak i obniżenie wskaźnika, o którym mowa w pkt. 1 względem wysokości tego wskaźnika z kwartału złożenia oferty o co najmniej 20 %,
- 3) zmiana wynagrodzenia może nastąpić najwcześniej w trzeciej dekadzie 7. miesiąca obowiązywania niniejszej Umowy,
- 4) zmiana wynagrodzenia nastąpi na podstawie wniosku o dokonanie waloryzacji wynagrodzenia wraz z uzasadnieniem wskazującym wysokość wskaźnika oraz przedmiot i wartość usług podlegających waloryzacji (niewykonanych do dnia złożenia wniosku), przy czym jedynie o 50% różnicy pomiędzy wskaźnikiem z kwartału waloryzacji, a wskaźnikiem z kwartału kiedy była złożona oferta. **Zmiana dotyczyć będzie wyłącznie płatności realizowanych po dniu złożenia wniosku,**
- 5) kolejna waloryzacja może nastąpić najwcześniej po upływie 3 miesięcy od dnia dokonania pierwszej waloryzacji,

- 6) warunkiem dokonania kolejnej waloryzacji jest comiesięczna zmiana cen dla danej kategorii na średnim poziomie 0,5% za dwa kolejne miesiące po dniu dokonania pierwszej waloryzacji,
- 7) zmiana wynagrodzenia nastąpi na podstawie wniosku o dokonanie waloryzacji wynagrodzenia wraz z uzasadnieniem wskazującym wysokość wskaźnika oraz przedmiot i wartość usług podlegających waloryzacji (niewykonanych do dnia złożenia wniosku).
- 8) zmiana wynagrodzenia wymaga pisemnego aneksu podpisanego przez obie Strony Umowy.
- 9) maksymalna wartość zmiany wynagrodzenia, jaką dopuszcza Zamawiający, to łącznie 2 % w stosunku do wartości całkowitego wynagrodzenia brutto określonego w § 7 ust. 1 umowy;
- 10) w przypadku, gdyby wskaźniki, o których mowa powyżej przestały być dostępne, zastosowanie znajdą inne, najbardziej zbliżone, wskaźniki publikowane przez Prezesa GUS.

7. Wykonawca, którego wynagrodzenie zostało zmienione zgodnie z ust. 1, zobowiązany jest do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę w zakresie odpowiadającym zmianom, o których mowa w ust. 1 (dotyczy to tylko faktur terminowo wystawionych po dniu złożenia wniosku).

§ 9

Odstąpienie od umowy

1. Zamawiający zastrzega prawo odstąpienia od umowy z Wykonawcą ze skutkiem natychmiastowym w przypadku rażących zaniedbań w wykonywaniu obowiązków Wykonawcy przewidzianych w umowie bądź wykonywania prac niezgodnie z umową.
2. Jeżeli Wykonawca będzie realizował przedmiot umowy wadliwie albo sprzecznie z umową, Zamawiający może wezwać go do zmiany sposobu wykonywania umowy i wyznaczyć mu w tym celu odpowiedni termin. Po bezskutecznym upływie wyznaczonego terminu Zamawiający może od umowy odstąpić, powierzyć poprawienie lub dalsze wykonanie przedmiotu umowy innemu podmiotowi na koszt Wykonawcy.

§ 10

Siła Wyższa

1. Żadna ze Stron Umowy nie będzie odpowiedzialna za niewykonanie lub nienależycie wykonanie zobowiązań wynikających z umowy, spowodowane przez okoliczności traktowane jako siła wyższa.
2. Siła wyższa oznacza zdarzenie zewnętrzne, nagłe, nieprzewidywalne i niezależne od woli Stron, uniemożliwiające wykonanie umowy w całości lub w części, na stałe lub pewien czas, któremu nie można zapobiec ani przeciwdziałać przy zachowaniu należytej staranności Stron. W szczególności strony traktują stan epidemii jako siłę wyższą.
3. W przypadku zaistnienia siły wyższej, Strona której taka okoliczność uniemożliwia lub utrudnia prawidłowe wywiązanie się z jej zobowiązań, powiadomi drugą stronę o takich okolicznościach i ich przyczynie.

§ 11
Postanowienia końcowe

1. Wykonawca nie może bez zgody Zamawiającego wyrażonej na piśmie pod rygorem nieważności, przenieść praw i obowiązków wynikających z Umowy na inny podmiot, w szczególności nie może dokonać cesji przysługujących mu wobec Zamawiającego wierzytelności.
2. Ewentualne spory cywilnoprawne wynikłe z niniejszej umowy Strony zobowiązują się poddać w sprawach, w których zawarcie ugody jest dopuszczalne, mediacjom lub innemu polubownemu rozwiązywaniu sporu przed Sądem Polubownym przy Prokuraturii Generalnej Rzeczypospolitej Polskiej, wybranym mediatorem albo osobą prowadzącą inne polubowne rozwiązanie sporu. W razie braku możliwości osiągnięcia porozumienia spory cywilnoprawne wynikłe w związku z realizacją niniejszej umowy, rozstrzygać będzie sąd właściwy dla siedziby Zamawiającego.
3. W okresie, w którym mogą być realizowane roszczenia z niniejszej Umowy, strony są zobowiązane informować się nawzajem na piśmie o każdej zmianie adresu swojego zamieszkania lub siedziby. W razie zaniedbania tego obowiązku korespondencję wysłaną na uprzednio wskazany adres listem poleconym za potwierdzeniem odbioru i nieodebraną, uważa się za doręczoną.
4. W sprawach nie unormowanych niniejszą umową mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r. — Kodeks cywilny (t. j. Dz. U. 2024 r. poz. 1061 ze zm.), ustawy z dnia 11 września 2019 r. — Prawo zamówień publicznych (t. j. Dz. U. 2024 poz. 1320) wraz z przepisami wykonawczymi.
5. Niniejszą Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron

ZAMAWIAJĄCY :

WYKONAWCA:

KONTRASYGNA TA SKARBNIKA:

**Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji
w Gminie Krobia w ramach projektu” Cyberbezpieczna Gmina Krobia”**

**Projekt współfinansowany przez Unię Europejską w ramach konkursu
grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane
usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu
cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA
ROZWÓJ CYFROWY 2021-2027 (FERC)**

Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów Informatycznych w Gminie Krobia poprzez opracowanie strategicznych i szczegółowych uregulowań w zakresie bezpieczeństwa informacji przez zaprojektowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, w tym Polityki Bezpieczeństwa Informacji dla jednostek podległych i przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa.

Jednostki podległe:

- Urząd Miejski w Krobi
- Centrum Usług Wspólnych w Krobi
- Miejsko Gminny Ośrodek Pomocy Społecznej w Krobi
- Szkoła Podstawowa im. Prof. Józefa Zwierzyckiego w Krobi
- Szkoła Podstawowa im. Ziemi Biskupiańskiej w Starej Krobi
- Zespół Szkolno- Przedszkolny w Pudliszkach
- Przedszkole Samorządowe pod Świerkami
- Żłobek Gminny w Krobi

Wykonawca musi zrealizować usługę polegającą na przeprowadzeniu audytu cyberbezpieczeństwa w ramach projektu „Cyberbezpieczny samorząd” zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 6 do Regulaminu Konkursu Grantowego „Cyberbezpieczny samorząd” zakończonego raportem oraz opracowaniem dokumentacji SZBI w oparciu o KRI/KSC i normę ISO27001.

Wykonanie i przekazanie Raportu z Audytu (opis zakresu przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytów, wnioski i zalecenia

związane z rozwiązaniem występujących problemów, analiza złożonego zał. nr 6 konkursu grantowego)

Informacje dotyczące infrastruktury w objętych jednostkach określa załącznik nr 1 do OPZ

ZAKRES ZAMÓWIENIA

Zaprojektowanie dokumentów, procedur i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym Polityki Bezpieczeństwa Informacji (PBI):

Etap I- Audyt Bezpieczeństwa Sieci

Etap II – opracowanie dokumentacji SZBI i PBI w tym Analiza Ryzyka oraz opracowanie planów ciągłości działania ;

Etap III – szkolenia z zakresu SZBI i PBI dla kierownictwa zamawiającego

Etap IV- szkolenia dot. Cyberbezpieczeństwa dla pracowników jednostek w kontekście wprowadzonego SZBI

Etap V – audyt powdrożeniowy.

Etap VI szkolenia dot. Cyberbezpieczeństwa dla pracowników jednostek w kontekście wprowadzonego SZBI

Oznaczenie przedmiotu zamówienia wg wspólnego słownika zamówień CPV

72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

72150000-1 Usługi doradztwa w zakresie audytu komputerowego oraz sprzętu komputerowego

72220000-3 Usługi doradcze w zakresie systemów i doradztwo techniczne

72254100-1 Usługi w zakresie testowania systemu

72500000-0 Komputerowe usługi pokrewne

72600000-6 Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego

72700000-7 Usługi w zakresie sieci komputerowej

72810000-1 Usługi audytu komputerowego

80000000-4 - Usługi edukacyjne i szkoleniowe

Opis Przedmiotu zamówienia:

ETAP I- Audyt bezpieczeństwa sieci w jednostkach

1. Audyt bezpieczeństwa Sieci- przeprowadzenie sprawdzenia bezpieczeństwa sieci polegającego na badaniu podatności sieci komputerowej na próby ataków pod kątem luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych oraz konfiguracji. Celem audytu jest określenie faktycznego stanu bezpieczeństwa struktur sieci LAN/ WAN oraz wykrycie naruszeń bezpieczeństwa sieci

ZAKRES DZIAŁAŃ:

Zamawiający oczekuje wykonania badania podatności sieci komputerowej na próby ataków pod kątem bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych oraz konfiguracji.

Podczas audytu Zamawiający oczekuje wykonania badań i analiz na wybranej próbie systemów i stacji roboczych określonych na początku audytu w zakresie:

- badania sieci pod kątem wykrytych adresów,
- wykonania testów sieci
i przygotowania rekomendacji do wykrytych podatności,
- dokonania analizy zasobów sieciowych i polityki haseł na stacjach i
przygotowania raportu zagrożeń z zaleceniami dotyczącymi zwiększenia bezpieczeństwa oraz rekomendacji w celu poprawy zagrożonych obszarów oraz dostarczenia ich do siedziby zamawiającego co najmniej w formie elektronicznej.

Zamawiający oczekuje sprawdzenia czy inwentaryzacja posiadanych licencji jest realizowana cyklicznie. Zamawiający oczekuje sprawdzenia liczby oraz typów licencji programów wykorzystywanych w organizacji, co pozwoli na sprawne wykrycie i usunięcie nielegalnego oprogramowania oraz na aktualizację oprogramowania, które jest niezbędne do funkcjonowania organizacji.

ZASADY WSPÓŁPRACY:

Zamawiający zapewnia pełny dostęp do sieci komputerowej audytorowi. Audyt nie obejmuje fizycznych zabezpieczeń infrastruktury informatycznej. Podczas audytu nie czyta się zawartości plików udostępnionych.

Zamawiający zapewnia pełny dostęp do wykazu oprogramowania i licencji audytorowi.

W celu potwierdzenia Zamawiający oczekuje raportu z audytu dostarczonego do Zamawiającego w formie papierowej lub elektronicznej opatrzonej podpisem kwalifikowanym .

Opracowanie raportu zawierającego wykryte podatności podzielone i przypisane, według wielkości zagrożenia. Raport powinien zawierać opis rekomendowanych działań zapobiegawczych zmierzających do wyeliminowania i/ lub ograniczenia podatności oraz wszelkich rozwiązań podnoszących poziom ochrony sieci.

Do badań podatności wykonawca musi używać oprogramowania komercyjnego, na które wykonawca przedstawi dowód licencyjny/zakupu oprogramowania.

Audyt będzie obejmował wszystkie jednostki :

Jednostka	Liczba audytów bezpieczeństwa sieci zgodnie z OPZ
Urząd Miejski w Krobi	1
Centrum Usług Wspólnych w Krobi	1
Miejsko Gminny Ośrodek Pomocy Społecznej w Krobi	1
Szkoła Podstawowa im. Prof. Józefa Zwierzyckiego w Krobi	1
Szkoła Podstawowa im. Ziemi Biskupiańskiej w Starej Krobi	1

Zespół Szkolno- Przedszkolny w Pudliszkach	1
Przedszkole Samorządowe pod Świerkami	1
Żłobek Gminny w Krobi	1
ŁĄCZNIE	8

informacje dotyczące infrastruktury w objętych jednostkach określa załącznik nr 1 do OPZ

ETAP II. Opracowanie i wdrożenie w jednostkach SZBI:

1. W ramach usługi wykonawca zobowiązany jest do opracowania/zaktualizowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji wraz z Polityką Bezpieczeństwa Informacji i przepisów wykonawczych w celu zgodności z prawem, i/lub podniesienia poziomu bezpieczeństwa informacji , zawierający niezbędne polityki i procedury w oparciu o:
 - a) Analizę poziomu spełnienia wymagań określonych w rozporządzeniu w sprawie Krajowych Ram Interoperacyjności oraz Ustawie o Krajowym Systemie Cyberbezpieczeństwa, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Krajowych Ram Interoperacyjności, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych w jednostkach,
 - b) Polską Normę PN-ISO/IEC 27001 oraz Polskie Normy związane z tą normą, w tym:
 - i) PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń;
 - ii) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem
 - c) Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
 - d) ustawę o Krajowym Systemie Cyberbezpieczeństwa,
 - e) dyrektywę NIS2,

- f) Rozporządzenie Parlamentu Europejskiego RODO, ustawę o informatyzacji podmiotów realizujących zadania publiczne

2. Wykonawca, na podstawie analizy obowiązany jest zaproponować organizację Systemu Zarządzania Bezpieczeństwem Informacji oraz opracować i przedstawić koncepcję wdrożenia Polityki Bezpieczeństwa Informacji w jednostkach.

Koncepcja będzie w szczególności zawierać:

- a) mapę dokumentów, stanowiącą szczegółowy wykaz dokumentów z zaznaczeniem ich wzajemnych powiązań, w tym:
- i) 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;
 - ii) Polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji w jednostkach w tym dla obszaru: teleinformatycznego, spraw osobowych, zabezpieczeń fizycznych, ciągłości działania, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa;
 - iii) Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

SZBI należy przygotować dla każdej wskazanej jednostki zgodnie z OPZ::

Jednostka	Liczba egz. opracowanej dokumentacji zgodnie z OPZ
Urząd Miejski w Krobi	1
Centrum Usług Wspólnych w Krobi	1
Miejsko Gminny Ośrodek Pomocy Społecznej w Krobi	1

Szkoła Podstawowa im. Prof. Józefa Zwierzyckiego w Krobi	1
Szkoła Podstawowa im. Ziemi Biskupiańskiej w Starej Krobi	1
Zespół Szkolno- Przedszkolny w Pudliszkach	1
Przedszkole Samorządowe pod Świerkami	1
Żłobek Gminny w Krobi	1
ŁĄCZNIE	8

Informacje dotyczące infrastruktury w objętych jednostkach określa załącznik nr 1 do OPZ

3. Stworzony lub zaktualizowany System Zarządzania Bezpieczeństwem powinien min. zawierać:
- Politykę Bezpieczeństwa Informacji
 - Procedury reagowania na incydenty (w tym określone w Ustawie o Krajowym Systemie Cyberbezpieczeństwa)
 - Procedury sprawdzania i aktualizacji dokumentacji
 - Procedury pracy na urządzeniach mobilnych i na odległość
 - Procedury awaryjnego odtwarzania systemów
 - Procedury wdrażania, likwidacji i inwentaryzacji sprzętu i oprogramowania
 - Procedury monitorowania, przeglądu i konserwacji systemów
 - Procedury przeprowadzania analizy ryzyka bezpieczeństwa informacji
 - Procedury sprawdzania i aktualizacji dokumentacji
 - Procedury nadawania/zmiany uprawnień
 - Procedury zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych
 - Procedury korzystania z systemów informatycznych
 - Procedury dot. odpowiedzialności i ról w zakresie utrzymywania SZBI

- Procedury zapewniające ochronę informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami
- Procedury szkoleń z bezpieczeństwa informacji
- Procedury zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie

Pozostałe procedury zostaną dopasowane do potrzeb jednostki oraz wewnętrznych regulacji i rozwiązań.

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.
 - a) Uwagi wniesione przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji wdrożenia SZBI i PBI.
 - b) Na podstawie zatwierdzonej przez Zamawiającego koncepcji Wykonawca opracuje wszystkie opisane w koncepcji dokumenty. Dokumenty muszą być zgodne ze wszystkimi wymaganiami prawnymi, którym podlegają jednostki.
 - c) Jeżeli w czasie realizacji umowy wymagania prawne w zakresie bezpieczeństwa informacji ulegną zmianie, Wykonawca zobowiązany jest dostosować dokumentację PBI do zaistniałych zmian.
 - d) Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego.

W Ramach opracowania i wdrożenia w jednostkach SZBI wykonawca dokona

Analizy Ryzyka, która obejmuje:

Zidentyfikowanie zagrożeń mogących wystąpić w Organizacji w zakresie ochrony danych i systemów informatycznych. Przeprowadzenie wywiadu z kierownikami poszczególnych komórek organizacyjnych lub osobami przez nich wyznaczone.

Weryfikacja dostarczonej dokumentacji. Usługa realizowana jest zgodnie z obowiązującymi przepisami prawa oraz zgodnie z normą PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem

Zakres działań obejmuje przeprowadzenie analizy ryzyka:

- Identyfikacja ryzyka dla poszczególnych czynności przetwarzania danych.
- identyfikacja zagrożeń dla poszczególnych czynności dotyczących danych osobowych oraz aktywów organizacji
- szacowanie ryzyka i konsekwencji jakie może ponieść organizacja w zakresie skutków prawnych, finansowych i wizerunkowych.
- Opracowanie raportu przedstawiającego ryzyko występujące w organizacji z ewentualnymi zaleceniami w celu poprawy bezpieczeństwa.

Wykonawca w ramach usługi:

udostępni narzędzie oraz opracuje metodykę przeprowadzenia analizy ryzyka przy współudziale wyznaczonych pracowników zamawiającego

A także dokona opracowania planów ciągłości działania dla kluczowych systemów IT co będzie polegało na :

Przeprowadzeniu wywiadu oraz analizy dokumentacji z zakresu bezpieczeństwa informacji. Stworzenie procedur, które będą stanowić dla Organizacji plany ciągłości działania obejmujące środki mające na celu minimalizację zakłóceń w działaniu systemów informatycznych, sieci, serwerów, baz danych itp. Dodatkowo także kwestie backupu danych, planów odtwarzania systemów, testowanie awaryjne, a także zarządzanie cyberzagrożeniami.

Przedstawieniu raportu z rekomendacjami oraz procedur zapewniających plan ciągłości działania w oparciu o normę 22301.

Na potwierdzenie realizacji wykonawca dostarczy :

- Dokumentację dotyczącą opracowanego/ zaktualizowanego Systemu Zarządzania Bezpieczeństwem Informacji zgodną z opisem przedmiotu zamówienia
- Raport przedstawiający ryzyko występujące w organizacji z ewentualnymi zaleceniami
- raport z rekomendacjami i oraz procedury zapewniających plan ciągłości działania w oparciu o normę 22301

Powyższe dokumenty należy przygotować dla każdej wskazanej jednostki zgodnie z OPZ::

Jednostka	Liczba egz.opracowanej dokumentacji zgodnie z OPZ
Urząd Miejski w Krobi	1
Centrum Usług Wspólnych w Krobi	1
Miejsko Gminny Ośrodek Pomocy Społecznej w Krobi	1
Szkoła Podstawowa im. Prof. Józefa Zwierzyckiego w Krobi	1
Szkoła Podstawowa im. Ziemi Biskupiańskiej w Starej Krobi	1
Zespół Szkolno- Przedszkolny w Pudliszkach	1
Przedszkole Samorządowe pod Świerkami	1
Żłobek Gminny w Krobi	1
ŁĄCZNIE	8

Informacje dotyczące infrastruktury w objętych jednostkach określa załącznik nr 1 do OPZ

Etap III – szkolenia z zakresu SZBI i PBI dla kierownictwa zamawiającego

Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkolenia z zakresu wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji dla kadry kierowniczej wskazanych jednostek, obejmujących co najmniej szkolenie :

- a) Podstawy prawne i główne zasady cyberbezpieczeństwa

- b) Wymogi wynikające z KRI, UoKSC i RODO
- c) Przegląd znanych typów ataków na JST - najnowsze zagrożenia informacji.
- d) Zarządzanie ryzykiem w bezpieczeństwie informacji
- e) System Zarządzania Bezpieczeństwem informacji – jak skutecznie przestrzegać procedur wdrożonej Polityki Bezpieczeństwa Informacji.
- f) Ciągłość działania – dlaczego jest istotna i jak ją wdrożyć
- g) Identyfikowanie zagrożeń – jak wdrożyć odpowiednie rozwiązania na przestrzeganie zasad bezpieczeństwa

Wymagania ogólne dla szkoleń:

Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).

Szkolenia będą trwały minimalnie 3 godziny a maksymalnie 7 godzin szkoleniowych w ciągu dnia.

Szkolenia będą odbywać się w dni robocze w godzinach 8.00 – 15.00.

Szkolenia będą prowadzone w języku polskim.

Dla kierowników jednostek 1 dzień szkoleniowy maksymalnie 20 osób

Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.

Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę, zgodnego z Ramowym zakresem szkolenia, znajdującym się powyżej.

Wykonawca zapewni co najmniej jedną 15 minutową przerwę dla każdej grupy.

W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.

Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie elektronicznej, zawierające szczegółowe

informacje, które będą omawiane podczas szkolenia. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na wskazane przez Zamawiającego adresy email. Dwa egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.

Właściwe działania promocyjne i informacyjne dotyczące szkoleń, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich zgodnie z wymaganiami konkursu grantowego „Cyberbezpieczny Samorząd”. współfinansowanego przez Unię Europejską w ramach konkursu grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC)

Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.

Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.

Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:

Lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).

Lista zaświadczeń o ukończeniu szkolenia.

Kserokopie zaświadczeń o ukończeniu szkolenia

Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie. Zamawiający dopuszcza dokument elektroniczny podpisany cyfrowo

Zamawiający zastrzega sobie prawo do rejestracji audiowizualnej przebiegu szkoleń.

Szkolenia należy wykonać po zakończeniu etapu II, nie później niż do końca 2025. roku

Wykonawca uzgodni termin szkolenia z zamawiającym nie później niż 30 dni przed planowanym terminem.

Etap IV Szkolenia dot. Cyberbezpieczeństwa dla pracowników jednostek w kontekście wprowadzonego SZBI

Szkolenia zostaną przeprowadzone w formie online.

1. Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń z zakresu Cyberbezpieczeństwa w kontekście wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji dla wskazanych pracowników jednostek, obejmujących co najmniej:
 - a) Bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI:
 - i) Wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa
 - ii) Wymagania dla pracowników wynikające z KRI, uoKSC oraz RODO
 - iii) System Zarządzania Bezpieczeństwem Informacji w praktyce
 - b) przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu:
 - i) Ochrona informacji i prywatność w internecie
 - ii) Ransomware jako poważne zagrożenie dla JST
 - iii) Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise)
 - iv) Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne
 - v) Bezpieczne hasła i uwierzytelnienie dwuskładnikowe
 - vi) Wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa

Wymagania ogólne dla szkoleń:

Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).

Szkolenia będą trwały minimalnie 3 godziny a maksymalnie 7 godzin szkoleniowych w ciągu dnia.

Szkolenia będą odbywać się w dni robocze w godzinach 8.00 – 15.00.

Szkolenia będą prowadzone w języku polskim.

Dla pracowników jednostek Wykonawca zaplanuje maksymalnie 3 dni szkoleniowe dla 6 grup (2 grupy dziennie) łącznie dla wszystkich jednostek, tj. maksymalnie 80 osób.

Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.

Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę, zgodnego z Ramowym zakresem szkolenia, znajdującym się powyżej.

Wykonawca zapewni co najmniej jedną 15 minutową przerwę dla każdej grupy.

W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.

Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie elektronicznej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na wskazane przez Zamawiającego adresy email. Dwa egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.

Właściwe działania promocyjne i informacyjne dotyczące szkoleń, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich zgodnie z wymaganiami konkursu grantowego „Cyberbezpieczny Samorząd”. współfinansowanego przez Unię Europejską w ramach konkursu grantowego pn. „Cyberbezpieczny Samorząd”,

Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC)

Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.

Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.

Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:

Lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).

Lista zaświadczeń o ukończeniu szkolenia.

Kserokopie zaświadczeń o ukończeniu szkolenia

Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie. Zamawiający dopuszcza dokument elektroniczny podpisany cyfrowo

Zamawiający zastrzega sobie prawo do rejestracji audiowizualnej przebiegu szkoleń.

W celu potwierdzenia realizacji zadania wykonawca dostarczy dokumentację z przeprowadzonych szkoleń opisaną w Opisie przedmiotu zamówienia

Szkolenia należy wykonać po zakończeniu etapu II, nie później niż do końca 2025.

Wykonawca uzgodni termin szkolenia z zamawiającym nie później niż 30 dni przed planowanym terminem.

ETAP V AUDYT POWDROŻENIOWY :

Wykonawca opracuje audyt powdrożeniowy, który będzie miał na celu przedstawienie Zamawiającemu postępu prac jaki został zrealizowany podczas wdrażania SZBI w poszczególnych jednostkach

Usługa będzie obejmować swoim zakresem:

1. **Audyt Systemu Zarządzania Bezpieczeństwem Informacji, audyt zgodności KRI/uoKSC:**

Przeprowadzenie audytu obejmuje wywiady z osobami kluczowymi dla ochrony informacji oraz weryfikację dokumentacji dotyczącej bezpieczeństwa informacji. Celem audytu jest ocena poziomu bezpieczeństwa informacji pod kątem zgodności z dobrymi praktykami oraz z wymaganiami określonymi w § 20 ust. 2 wspomnianego rozporządzenia KRI lub z normą PN-ISO/IEC 27001.

Badaniem jest objęta:

- Dokumentacja bezpieczeństwa.
- Role w organizacji.
- Zarządzanie ryzykiem.
- Świadomość użytkowników.
- Doskonalenie.
- Organizacja bezpieczeństwa informacji.
- Bezpieczeństwo zasobów ludzkich.
- Zarządzanie aktywami.
- Kontrola dostępu.
- Kryptografia.
- Bezpieczeństwo fizyczne i środowiskowe.
- Bezpieczna eksploatacja.
- Bezpieczeństwo komunikacji.

- Pozyskiwanie rozwój i utrzymywanie systemów.
- Relacje z dostawcami.
- Zarządzanie incydentami.
- Zarządzanie ciągłością działania.
- Zgodności z prawem.

Przedstawienie raportu pozwalającego stwierdzić Zamawiającemu, na jakim poziomie jest zarządzanie bezpieczeństwem informacji oraz jakie obszary powinien jeszcze doskonalić, aby osiągnąć gotowość do wdrożenia dobrych praktyk w oparciu o normę ISO 27001, rozporządzenie KRI oraz ustawę o Krajowym Systemie Cyberbezpieczeństwa.

Audyt musi zostać przeprowadzony przez podmiot/osobę posiadający/ą przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999);

Po zakończeniu audytu Wykonawca przygotowuje i przekazuje w formie papierowej lub elektronicznej opatrzonej podpisem kwalifikowanym raport z przeprowadzonego audytu i naniesie dane do ankiety wskazanej w załączniku nr 6 do regulaminu konkursu.

Audyt zostanie przeprowadzony dla każdej jednostki wskazanej w OPZ:

Jednostka	Liczba audytów powdrożeniowych zgodnych z OPZ
Urząd Miejski w Krobi	1
Centrum Usług Wspólnych w Krobi	1
Miejsko Gminny Ośrodek Pomocy Społecznej w Krobi	1

Szkoła Podstawowa im. Prof. Józefa Zwierzyckiego w Krobi	1
Szkoła Podstawowa im. Ziemi Biskupiańskiej w Starej Krobi	1
Zespół Szkolno- Przedszkolny w Pudliszkach	1
Przedszkole Samorządowe pod Świerkami	1
Żłobek Gminny w Krobi	1
ŁĄCZNIE	8

Informacje dotyczące infrastruktury w objętych jednostkach określa załącznik nr 1 do OPZ

Etap VI szkolenia dot. Cyberbezpieczeństwa dla pracowników jednostek w kontekście wprowadzonego SZBI

Szkolenia zostaną przeprowadzone w formie online.

1. Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń z zakresu Cyberbezpieczeństwa w kontekście wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji dla wskazanych pracowników jednostek, obejmujących co najmniej:
 - a) Bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI:
 - i) Wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa
 - ii) Wymagania dla pracowników wynikające z KRI, uoKSC oraz RODO
 - iii) System Zarządzania Bezpieczeństwem Informacji w praktyce
 - b) Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu:
 - i) Ochrona informacji i prywatność w internecie

- ii) Ransomware jako poważne zagrożenie dla JST
- iii) Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise)
- iv) Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne
- v) Bezpieczne hasła i uwierzytelnienie dwuskładnikowe
- vi) Wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa

Wymagania ogólne dla szkoleń:

Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).

Szkolenia będą trwały minimalnie 3 godziny a maksymalnie 7 godzin szkoleniowych w ciągu dnia.

Szkolenia będą odbywać się w dni robocze w godzinach 8.00 – 15.00.

Szkolenia będą prowadzone w języku polskim.

Dla pracowników jednostek Wykonawca zaplanuje maksymalnie 3 dni szkoleniowe dla 6 grup (2 grupy dziennie) łącznie dla wszystkich jednostek, tj. maksymalnie 80 osób.

Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.

Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę, zgodnego z Ramowym zakresem szkolenia, znajdującym się powyżej.

Wykonawca zapewni co najmniej jedną 15 minutową przerwę dla każdej grupy.

W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.

Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty

informacyjne, broszury) w formie elektronicznej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na wskazane przez Zamawiającego adresy email. Dwa egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.

Właściwe działania promocyjne i informacyjne dotyczące szkoleń, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich zgodnie z wymaganiami konkursu grantowego „Cyberbezpieczny Samorząd”. współfinansowanego przez Unię Europejską w ramach konkursu grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC)

Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.

Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.

Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:

Lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).

Lista zaświadczeń o ukończeniu szkolenia.

Kserokopie zaświadczeń o ukończeniu szkolenia

Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie. Zamawiający dopuszcza dokument elektroniczny podpisany cyfrowo

b) Zamawiający zastrzega sobie prawo do rejestracji audiowizualnej przebiegu szkoleń.

W celu potwierdzenia realizacji zadania wykonawca dostarczy dokumentację z przeprowadzonych szkoleń opisaną w Opisie przedmiotu zamówienia

Wykonawca przedstawi harmonogram realizacji zadania uzgodniony z wykonawcą do 7 dni od podpisania umowy.

Zamawiający dopuszcza płatności częściowe na podstawie częściowego protokołu odbioru po wykonaniu poszczególnych etapów wskazanych w OPZ i dostarczeniu dokumentów potwierdzających ich realizację.

Załącznik nr 1 do OPZ- informacje dotyczące infrastruktury w objętych jednostkach

Informacje:	Liczba/szt.: Urząd Miejski	Liczba /szt.: MGOPS	Liczba /szt.: CUW	Liczba /szt.: SP Krobia	Liczba /szt.: ZSP Pudliszki	Liczba /szt.: SP Stara Krobia	Liczba /szt.: Żłobek Gminny	Liczba /szt.: Przedszkole Pod Świerkami
Liczba lokalizacji działalności organizacji	2	1	1	4	4	2	1	3
Liczba serwerów fizycznych	4	1	1	1	2	2	0	0
Liczba serwerów wirtualnych	2	0	0	0	4	1	0	0
Liczba zewnętrznych adresów IP	1	1	0	1	0	0	0	0

Informacje:	Liczba /szt.: Urząd Miejski	Liczba /szt.: MGOPS	Liczba /szt.: CUW	Liczba /szt.: SP Krobia	Liczba /szt.: ZSP Pudliszki	Liczba /szt.: SP Stara Krobia	Liczba /szt.: Żłobek Gminny	Liczba /szt.: Przedszkole Pod Świerkami
1. stacji roboczych	1. 35 2. 12	1. 15 2. 8	1. 11 2. 3	1. 72 2. 5	1. 62 2. 14 (w tym 4 wynajem)	1. 47 2. 8	1. 2 2. 2	1. 12 2. 3
2. drukarki sieciowe	3. 1 4. 5	3. 1 4. 3	3. 1 4. 1	3. 2 4. 5	3. 4	3. 2(1 Stara Krobia, 1 Sułkowice)	3. 1 4. 1	3. 1 4. 1
3. routery	5. -	5. -	5. 0	5. 0	4. 10		5. 0	5. 0
4. switch-e	6. 4	6. 2	6. 3	6. 21	5. 4	4. 5	6. 0	6. 6
5. modem	7. 1	7. 1	7. 1	7. 0	6. 14 (w tym 3 nie połączone)	5. 0 6. 8 7. 0	7. 0	7. 0
6. access point								

7. UTM					7. 0			
--------	--	--	--	--	------	--	--	--