



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Załącznik nr 1

Opis Przedmiotu Zamówienia

Opracowywanie oraz wdrożenie

Systemu Zarządzania

Bezpieczeństwem Informacji



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

I.	WYMAGANIA OGÓLNE.....	4
II.	WYMAGANIA MINIMALNE OPRACOWANIA ORAZ WDROŻENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	4
III.	TERMIN REALIZACJI ZAMÓWIENIA	6



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



WSTĘP

Niniejszy załącznik określa minimalne wymagania dla opracowania oraz wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji dla Starostwa Powiatowego w Wągrowcu i jednostek podległych realizowanego w ramach „Cyberbezpieczny Samorząd” dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego.



I. WYMAGANIA OGÓLNE

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do opracowywania oraz wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji [SZBI] dla:

1. Starostwo Powiatowe w Wągrowcu
2. Jednostka podległa:
 - a) Powiatowy Urząd Pracy w Wągrowcu
 - b) Powiatowy Zarząd Dróg w Wągrowcu
 - c) Powiatowe Centrum Pomocy Rodzinie w Wągrowcu
 - d) Dom Pomocy Społecznej w Srebrnej Górze
 - e) I Liceum Ogólnokształcące im. Powstańców Wielkopolskich
 - f) Zespół Szkół nr 1 w Wągrowcu
 - g) Zespół Szkół nr 2 im. ppłk. dr. Stanisława Kulińskiego
 - h) Zespół Szkół im. Karola Libelta w Gołanicy
 - i) Młodzieżowy Ośrodek Wychowawczy im. Janusza Korczaka
 - j) Młodzieżowy Ośrodek Socjoterapii w Gołanicy im. Kompanii Gołanieckiej
 - k) Specjalny Ośrodek Szkolno-Wychowawczy im. Janusza Korczaka
 - l) Bursa Szkolna nr 1
 - m) Poradnia Psychologiczno-Pedagogiczna
 - n) Ognisko Pracy Pozaszkolnej
 - o) Placówka Opiekuńczo Wychowawcza w Wągrowcu

wg poniższych wymagań minimalnych.

II. WYMAGANIA MINIMALNE OPRACOWANIA ORAZ WDROŻENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Nazwa	Minimalne wymagania dla usługi
Typ	Wykonanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji [SZBI] zgodnie z wytycznymi normy PN-EN ISO/IEC 27001
Zakres dokumentacji	W ramach zamówienia wymagane jest przygotowanie dokumentacji w zakresie minimalnym: <ul style="list-style-type: none"> • Polityka Bezpieczeństwa Informacji • Polityka ochrony danych osobowych – dostosowanie obowiązującego dokumentu do potrzeb wdrażanej dokumentacji SZBI. • Polityka zarządzania systemem informatycznym • Polityka zarządzania ciągłością działania • Procedura zarządzania incydentami cyberbezpieczeństwa lub jej aktualizacja • Analiza ryzyka w zakresie Bezpieczeństwa Informacji
Wymagane procedury	W ramach poszczególnych elementów SZBI wymagane jest wdrożenie niezbędnych procedur w zakresie minimalnym, zgodnych z przepisami prawa, które są powszechnie obowiązujące: <ul style="list-style-type: none"> • Procedury korzystania z urządzeń mobilnych



	<ul style="list-style-type: none">• Procedury pracy zdalnej• Postępowanie z nośnikami• Procedury kontroli dostępu• Zabezpieczenie pomieszczeń i obiektów• Procedury czystego biurka• Procedury czystego ekranu• Procedury kopii zapasowych• Procedury ochrony logów• Bezpieczeństwo komunikacji• Zarządzanie bezpieczeństwem sieci• Przesyłanie informacji• Plany ciągłości działania• Procedury zarządzania incydentami• Prywatność i ochrona danych osobowych• Szacowanie ryzyka w obszarze bezpieczeństwa informacji• Szkolenia personelu• Plan zarządzania podatnościami• Plan reagowania na incydenty• Plan przywracania <p>Zamawiający zastrzega sobie prawo wnoszenia uwag do zaproponowanego SZBI, w tym do rodzaju dokumentów, zakresu merytorycznego itp.</p> <p>Wykonawca gwarantuje, że opracowana przez niego dokumentacja systemu zarządzania bezpieczeństwem informacji będzie zgodna z obowiązującymi przepisami prawa.</p>
Wsparcie przed i powdrożeniowe	<p>Zamawiający wymaga, aby w ramach wdrożenia Wykonawca także:</p> <ul style="list-style-type: none">- świadczył usługę asysty w zakresie 16 roboczogodzin przy wdrażaniu dokumentacji SZBI. Usługi asysty mogą być świadczone zdalnie lub w siedzibie Zamawiającego. <p>Dodatkowo Zamawiający wymaga, aby:</p> <ul style="list-style-type: none">- zakres wdrożenia dokumentacji SZBI obejmował wytyczne wynikające z raportu z przeprowadzonego audytu wstępnego posiadanej przez Zamawiającego dokumentacji;- bezpłatnie zaktualizował dokumentację według zaleceń wynikających z przeprowadzonego raportu z audytu końcowego przeprowadzonego po wdrożeniu dokumentacji SZBI.
Szkolenie	<p>W ramach realizacji usługi Zamawiający wymaga dodatkowego szkolenia w ramach SZBI, realizowanego za pośrednictwem symulatora zagrożeń internetowych. Wymagania minimalne dla szkolenia:</p> <ol style="list-style-type: none">1. Zamawiający wymaga, aby Wykonawca w ramach realizacji szkolenia przedstawił Zamawiającemu czytelne zasady obsługi symulatora.2. Zamawiający wymaga, aby szkolenie w ramach symulatora umożliwilo bezpieczny sposób sprawdzenia oraz poznania typowych zagrożeń występujących w obszarze przestrzeni internetowej na dedykowanej platformie dostępnej na stronie www. dostosowanej do standardu min. WCAG 2.1, bez możliwości zapisu oraz archiwizacji wprowadzonych danych.



	<p>3. Zamawiający wymaga, aby realizacja szkolenia odbyła się wg szkoleniowych scenariuszy zagrożeń popularnych przestępstw internetowych w zakresie minimum:</p> <ul style="list-style-type: none">• Phishing Clone,• PhishingSpear,• PhishingSpear Chat,• PhishingWhaling,• Pharming,• Malware Post,• Malware Email• Certificate Fraud <p>4. Zamawiający wymaga, aby w ramach szkolenia miał nieograniczony dostęp do modułów szkoleniowych w zakresie SZBI spełniających poniższe możliwości:</p> <ul style="list-style-type: none">• Moduł podstron (fałszywych witryn) do tworzenia witryn nakłaniających do pobierania zainfekowanych załączników, podawania wrażliwych danych lub dokonywania płatności internetowych.• Moduł czatu z botami, symulujący wyłudzenia danych osobowych i numerów kart kredytowych.• Moduł e-mail do przeglądania wiadomości z linkami lub załącznikami, symulującymi działanie malware.• Moduł edukacyjny z informacjami o cyberprzestępstwach, identyfikacji zagrożeń, sposobach zapobiegania i działania po oszustwie.• Moduł postów społecznościowych, prezentujący potencjalne ataki phishingowe lub pharmingowe. <p>Zamawiający wymaga dostępu do szkolenia przez okres minimum 6 miesięcy od daty podpisania umowy.</p>
Wymagania dodatkowe	<p>Zamawiający wymaga, aby Wykonawca posiadał wdrożone normy ISO 22301 oraz 27001 lub normy równoważne.</p> <p><u>Na potwierdzenie spełniania warunku wymagane jest dołączenie dokumentów potwierdzających posiadanie certyfikacji do oferty.</u></p>
Ilość	16 szt.

III. TERMIN REALIZACJI ZAMÓWIENIA

Zamawiający wymaga, aby przedmiot niniejszego zapytania został wykonany w terminie do 75 dni od daty podpisania umowy z Wykonawcą.