



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 DLA UG	4
III.	WYMAGANIA MINIMALNE OPRACOWANIA ORAZ WDROŻENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI DLA JP	6
IV.	TERMIN REALIZACJI ZAMÓWIENIA	7



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 Gminy Bielawa 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:

- a) Urzędu Gminy w Bielawie [UG] - 1 szt.
- b) Jednostek podległych [JP] – 8 szt.
 - Ośrodek Pomocy Społecznej,
 - Zespół Ośrodków Wsparcia,
 - Miejski Ośrodek Kultury i Sztuki,
 - Szkoła Podstawowa nr 7 im. Juliana Tuwima,
 - Miejski Zarząd Placówek Oświaty,
 - Żłobek Publiczny nr 2,
 - Straż Miejska,
 - Ośrodek Sportu i Rekreacji.

II. WYMAGANIA MINIMALNE OPRACOWANIA ORAZ WDROŻENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI DLA UG

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: • 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: • Procedury korzystania z urządzeń mobilnych • 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 Zamawiający zastrzega sobie prawo wnoszenia uwag do zaproponowanego SZBI, w tym do rodzaju dokumentów, zakresu merytorycznego itp. Wykonawca gwarantuje, że opracowana przez niego dokumentacja systemu zarządzania bezpieczeństwem informacji będzie zgodna z obowiązującymi przepisami prawa.
Wsparcie przy wdrożeniu	Wykonawca będzie świadczył usługę asysty w zakresie 16 roboczogodzin przy wdrażaniu dokumentacji SZBI. Usługi asysty mogą być świadczone zdalnie lub w siedzibie Zamawiającego w okresie od daty podpisania umowy do 30-06-2026 r.
Szkolenie	W ramach realizacji usługi Zamawiający wymaga dodatkowego szkolenia w ramach SZBI, realizowanego za pośrednictwem symulatora zagrożeń internetowych. Wymagania minimalne dla szkolenia: 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. 3. Zamawiający wymaga, aby realizacja szkolenia odbyła się wg szkoleniowych scenariuszy zagrożeń popularnych przestępstw internetowych w zakresie minimum: • Phishing Clone, • PhishingSpear, • PhishingSpear Chat, • PhishingWhaling, • Pharming, • Malware Post, • Malware Email • Certificate Fraud



	4. Zamawiający wymaga, aby w ramach szkolenia miał nieograniczony dostęp do modułów szkoleniowych w zakresie SZBI spełniających poniższe możliwości: · 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. Zamawiający wymaga dostępu do szkolenia przez okres minimum 6 miesięcy od daty podpisania umowy.
Wymagania dodatkowe	Zamawiający wymaga, aby Wykonawca posiadał wdrożone normy ISO 22301 oraz 27001 lub normy równoważne. <u>Na potwierdzenie spełniania warunku wymagane jest dołączenie dokumentów potwierdzających posiadanie certyfikacji do oferty.</u>
Ilość	1 szt.

III. WYMAGANIA MINIMALNE OPRACOWANIA ORAZ WDROŻENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI DLA JP

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: • 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: • Procedury korzystania z urządzeń mobilnych • 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 Zamawiający zastrzega sobie prawo wnoszenia uwag do zaproponowanego SZBI, w tym do rodzaju dokumentów, zakresu merytorycznego itp. Wykonawca gwarantuje, że opracowana przez niego dokumentacja systemu zarządzania bezpieczeństwem informacji będzie zgodna z obowiązującymi przepisami prawa.
Wsparcie przy wdrożeniu	Wykonawca będzie świadczył usługę asysty w zakresie 16 roboczogodzin przy wdrażaniu dokumentacji SZBI. Usługi asysty mogą być świadczone zdalnie lub w siedzibie Zamawiającego w okresie od daty podpisania umowy do 30-06-2026 r.
Wymagania dodatkowe	Zamawiający wymaga, aby Wykonawca posiadał wdrożone normy ISO 22301 oraz 27001 lub normy równoważne. <u>Na potwierdzenie spełniania warunku wymagane jest dołączenie dokumentów potwierdzających posiadanie certyfikacji do oferty.</u>
Ilość	8 szt.

IV. TERMIN REALIZACJI ZAMÓWIENIA

Zamawiający wymaga, aby przedmiot niniejszego zapytania został wykonany w terminie do 90 dni od daty podpisania umowy z Wykonawcą.