



Załącznik nr 1 do zapytania ofertowego

Opis przedmiotu zamówienia dotyczący

Wykonanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji [SZBI]

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do: **wykonania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji [SZBI] dla:**

- a) Urząd Gminy Krzęcin
- b) Ośrodek Pomocy Społecznej w Krzęcinie oraz

Lp.	Nazwa komponentu	Wymagane minimalne dla usług
1	2	3
1.	Typ	Wykonanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji [SZBI] zgodnie z wytycznymi normy PN-EN ISO/IEC 27001
2.	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 • Analiza ryzyka w zakresie Bezpieczeństwa Informacji
3.	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.
4.	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.
5.	Wymagania dodatkowe	W ramach realizacji usługi Zamawiający wymaga dodatkowego wsparcia systemem zapewniającym zaawansowane zabezpieczenie technologiczne, w postaci: • MONITOROWANIA CYBERBEZPIECZEŃSTWA w sposób ciągły i proaktywny - o <u>Monitorowanie od strony sieci Internet otwartych portów i usług</u> – ponieważ otwarte porty i dostępne usługi mogą stać się celem ataków, ich monitorowanie jest kluczowym elementem zarządzania bezpieczeństwem sieci. Funkcja monitorowania umożliwia szybkie wykrycie, jeśli porty zostaną otwarte bez autoryzacji lub jeśli usługi zostaną uruchomione na urządzeniach, co może sugerować naruszenie bezpieczeństwa. • WYKRYWANIA PODATNOŚCI w czasie rzeczywistym - o <u>Indeksowanie podatności w urządzeniach podłączonych do Internetu</u> – Funkcja ta daje użytkownikom usługi możliwość natychmiastowego otrzymywania powiadomień o nowych podatnościach wykrytych w ich infrastrukturze. To z kolei pozwala na szybkie działania zapobiegawcze, takie jak instalacja poprawek bezpieczeństwa lub ograniczenie dostępu do podatnych urządzeń. • ANALIZY ZAGROŻEŃ ZWIĄZANYCH Z IoT - o <u>Analiza zagrożeń związanych z IoT</u> – jest szczególnie przydatna w kontekście monitorowania urządzeń Internetu Rzeczy (IoT), które często są słabo zabezpieczone. Dzięki monitorowaniu tych urządzeń za pomocą usługi, organizacje mogą skuteczniej zarządzać ryzykiem, jakie niesie ze sobą IoT, a także minimalizować potencjalne wektory ataku. • POWIADOMIEŃ O ZMIANACH W INFRASTRUKTURZE - o Jednym z kluczowych aspektów cyberbezpieczeństwa jest świadomość zmian w infrastrukturze IT. System wysyła powiadomienia, gdy do sieci zostają dodane nowe urządzenia, co może być sygnałem

	potencjalnych zagrożeń lub naruszeń. Pozwala to na szybkie zbadanie i, jeśli to konieczne, zabezpieczenie tych nowych elementów. • WSPARCIA DLA PROAKTYWNEJ OBRONY o Zamiast reagować na incydenty już po ich wystąpieniu, system umożliwia stosowanie proaktywnych środków bezpieczeństwa. Regularne analizy danych pomagają zidentyfikować anomalie lub potencjalne ataki, zanim te doprowadzą do rzeczywistych szkód. • ZGODNOŚCI Z PRZEPISAMI PRAWA o Wspomaga organizację w utrzymaniu zgodności z regulacjami dotyczącymi ochrony danych osobowych, bezpieczeństwa informacji i cyberbezpieczeństwa, np. RODO, Ustawy o Krajowym Systemie Cyberbezpieczeństwa, Rozporządzenia o Krajowych Ram Interoperacyjności poprzez dostarczanie dokładnych i bieżących danych o stanie bezpieczeństwa infrastruktury IT. System może być także użyteczny w audytach bezpieczeństwa, dostarczając dokumentację zmian i zagrożeń. Świadczenie usługi wsparcia systemem obejmuje okres 6 miesięcy. Dodatkowo Zamawiający wymaga udostępnienia symulatora zagrożeń internetowych w zakresie minimum : 1. Czytelne zasady obsługi - przedstawione w ramach zorganizowanego szkolenia oraz opisane w dołączonej instrukcji. 2. Bezpieczny sposób sprawdzenia oraz poznania typowych zagrożeń występujących w obszarze przestrzeni internetowej na dedykowanej platformie dostępnej na stronie www. dostosowanej do standardu WCAG 2.1, bez możliwości zapisu oraz archiwizacji wprowadzonych danych. 3. Realizację minimum ośmiu scenariuszy zagrożeń popularnych przestępstw internetowych typu: Phishing Clone, PhishingSpear, PhishingSpear Chat, PhishingWhaling, Pharming, Malware Post, Malware Email. 4. Możliwość tworzenia nowych scenariuszy zagrożeń w obszarze cyberbezpieczeństwa. 5. Nieograniczony dostęp do modułów 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. 6. Opracowanie oraz przekazanie zestawu testowego potwierdzającego
--	---



		funkcjonalność SYMULATORA poprzez: · dokonanie prezentacji oferowanego Systemu Symulatora zagrożeń internetowych w obszarach proponowanych scenariuszy. Świadczenie usługi Symulatora Zagrożeń Internetowych obejmuje okres 6 miesięcy.
--	--	--

I. TERMIN REALIZACJI ZAMÓWIENIA:

Zamawiający wymaga, aby przedmiot niniejszego zapytania został wykonany w terminie do 3 miesięcy od daty podpisania umowy z Wykonawcą.

GMINA KRZĘCIN
ul. Tylna 7, 73-231 Krzęcin
tel./fax 095 765 52 13
NIP 5941528641, REGON 210966987

WÓJT GMINY KRZĘCIN

dr Bogdan Wojciech Brzustowicz