Załącznik nr 1 do zapytania ofertowego

Szczegółowy opis przedmiotu zamówienia (SOPZ)

Spis przedmiotu zamówienia:
1. Szkolenie dla pracowników samorządowych w zakresie cyberbezpieczeństwa
2. Diagnoza cyberbezpieczeństwa

1. Szkolenie dla pracowników samorządowych w zakresie cyberbezpieczeństwa

Lp.	Parametr	WYMAGANE MINIMALNE PARAMETRY PLANOWANEGO ZAMÓWIENIA
1.	Typ	**Szkolenie zdalne bądź stacjonarne dla pracowników Urzędu z zakresu cyberbezpieczeństwa.**
2.	**Wymagany minimalny zakres szkolenia**	1. Wprowadzenie do bezpieczeństwa informacji w oparciu o Normę ISO/IEC 27001:2017-06 2. Przepisy regulujące ochronę danych: RODO i Ustawa o ochronie danych osobowych 3. Ustawa o krajowym systemie cyberbezpieczeństwa i podstawowe definicje, 4. Podział ról i obowiązków wynikających z przepisów prawa, 5. Praktyczne zasady zapewniania bezpieczeństwa informacji, 6. Kontrola dostępu fizycznego, zarządzanie kluczami 7. Zasady bezpiecznej eksploatacji sprzętu i oprogramowania, 8. Zasada czystego biurka i czystego pulpitu, 9. Cyberbezpieczeństwo w praktyce, 10. Informacje uwierzytelniające, logowanie do sieci, 11. Praca zdalna - czym jest VPN i jak z niego korzystać, 12. Korzystanie z Internetu i poczty elektronicznej. Przedstawienie przykładów i nauka rozpoznawania niepożądanych maili i ich zawartości, 13. Darmowe WiFi i automatyczne podłączanie się, 14. Ataki socjotechniczne, 15. Postępowanie z naruszeniami bezpieczeństwa informacji, 16. Skutki naruszeń i konsekwencje prawne 17. Dlaczego wiedza o cyberbezpieczeństwie jest konieczna? 18. Sposoby ochrony kont i danych przed potencjalnym zagrożeniem. 19. Częsta zmiana haseł, czy ustalanie ich odpowiedniej trudności a co za tym idzie programy pomagające w tym 20. Opis Certyfikatów stron internetowych. 21. Wprowadzenie do sieci komputerowych - niebezpieczeństwo sieci otwartych bezprzewodowych. 22. Niezabezpieczone protokoły sieciowe - HTTP FTP

Lp.	Parametr	WYMAGANE MINIMALNE PARAMETRY PLANOWANEGO ZAMÓWIENIA
1.	Typ	**Szkolenie zdalne bądź stacjonarne dla pracowników Urzędu z zakresu cyberbezpieczeństwa.**
		23. Zaszyfrowana komunikacja w Internecie (komunikatory) 24. Ochrona plików i dysków czyli podstawy szyfrowania. 25. Odpowiednia weryfikacja odbiorcy i nadawcy. 26. Weryfikacją wiadomości e-mail 27. Weryfikacja i skan plików znajdujących się w załączniku. 28. Przykłady ataków oraz sposoby na ochronę przed nimi pod kątem zwykłego użytkownika 29. Phishing - Sposoby na zabezpieczenie się przed włamaniami i oszustwem w sieci 30. Programy antywirusowe i ich rola (omówienie popularnych programów i opis ich działania) 31. Tworzenie kopii zapasowych i ich odzyskiwanie po awarii. 32. Sposoby tworzenia backupów. 33. Podpis elektroniczny dokumentów w prosty i bezpieczny sposób.
	Wymagania dodatkowe	W ramach realizacji szkolenia wymagane jest, aby: – Szczegółowy harmonogram i tematyka szkolenia został uzgodniony z Zamawiającym w terminie minimum 14 dni przed terminem rozpoczęcia szkolenia – Szkolenia zostaną przeprowadzone w maksymalnie 2 turach po minimum 3 godziny, – Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych, – Uczestnik po zakończeniu szkolenia musi otrzymać zaświadczenie ukończenia szkolenia, – Uczestnik musi mieć możliwość bezpłatnego 14-sto dniowego kontaktu z trenerem po szkoleniu.
	Ilość osób do przeszkolenia	Szkolenie dla 100 pracowników

2. <u>Diagnoza cyberbezpieczeństwa:</u>

Przeprowadzona zgodnie z zakresem oraz formularzem stanowiącym załącznik pn.: *„Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa”* (w załączeniu) przez osobę posiadająca uprawnienia wykazane w *Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.*

Diagnozę cyberbezpieczeństwa należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.

Załączniki do opisu diagnozy cyberbezpieczeństwa:

– Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa
– Rozporządzenie Mini. Cyfryzacji wykaz certyfikatów uprawniających do przeprowadzenia audytu

Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa

1. Audyt bezpieczeństwa danych w systemach informatycznych oraz sieci ICT w oparciu o KRI i KSC:
   1.1. Analiza wszystkich zabezpieczeń przed utratą i kradzieżą danych
   1.2. Analiza kontroli dostępu do systemów informatycznych w tym dostępu przez usługi i narzędzia zdalne
   1.3. Analiza zabezpieczeń przy pracy zdalnej
   1.4. Analiza i ocena technicznej infrastruktury w systemach ICT, schematu sieci a także technicznych zabezpieczeń sieci
   1.5. Analiza i ocena zabezpieczeń dostępu do sieci publicznej
   1.6. Analiza i ocena zabezpieczeń wewnętrznej sieci ICT
   1.7. Ocena sposobu identyfikowania i logowania użytkowników
   1.8. Sprawdzenie zabezpieczeń komputerów przed atakami phishingowymi
   1.9. Weryfikacja systemu uwierzytelniania użytkowników i administratorów
   1.10. Weryfikacja systemu uwierzytelniania użytkowników i administratorów do systemu operacyjnego i kontrolera domeny
   1.11. Sprawdzenie sposobów i systemów szyfrowania m.in. protokoły szyfrowania, szyfrowanie danych END-to-END w poczcie email itp.
   1.12. Analiza i ocena sposobu zbierania logów, zakresu i retencji logów
   1.13. Kontrola systemu monitoringu
   1.14. Kontrola systemu alarmowego
   1.15. Analiza i ocena procedur zarządzania systemami teleinformatycznymi
   1.16. Analiza i ocena ochrony ICT przed oprogramowaniem szkodliwym, w tym weryfikacja zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania
   1.17. Analiza i ocena procedur historii zmian w dokumentach, systemach informatycznych itp.
   1.18. Analiza i ocena procedur zarządzania i zabezpieczania nośników przechowujących dane
   1.19. Analiza i ocena zasad odpowiedzialności użytkowników
   1.20. Analiza i ocena zasad zarządzania hasłami
   1.21. Analiza i ocena zabezpieczeń kryptograficznych
   1.22. Analiza i ocena zabezpieczeń komputerów przenośnych w tym praca zdalna.
   1.23. Analiza stopnia zabezpieczenia stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe
   1.24. Analiza i ocena niszczenia niepotrzebnych nośników oraz danych
   1.25. Analiza i ocena ciągłości pracy systemów i sieci ICT
   1.26. Analiza i ocena systemów backupów i archiwizacji danych w tym testy odtworzeniowe
      1.26.1. Weryfikacja i ocena procedur wykonywania kopii zapasowych zawartych w dokumentacji bezpieczeństwa
      1.26.2. Weryfikacja i ocena wykazów, logów świadczących o realizacji zadań zgodnie z przyjętymi zapisami w polityce
      1.26.3. Weryfikacja zasobów do wykonywania testów odtworzeniowych
      1.26.4. Weryfikacja czy są wykonywane testowe odtworzenia
2. Testy penetracyjne systemów informatycznych i całej infrastruktury ICT
   2.1. Testy styku sieci lokalnej z Internetem przeprowadzane ze stacji roboczej podłączonej do sieci Internet
      - Analiza topologii brzegu sieci
      - Weryfikacja mechanizmów ochronnych
      - Próba wykrycia usług sieciowych udostępnianych do Internetu
      - Detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet

Postępowanie o udzielenie zamówienia publicznego jest prowadzone zgodnie z „Regulaminem zamówień publicznych" określającym zasady i sposób postępowania przy udzielaniu zamówień o wartości poniżej 130.000,00 PLN stanowiącym załącznik nr 1 do Zarządzenia Nr 33/2021 Wójta Gminy Dobrcz z dnia 1 czerwca 2021 r. w strawie wprowadzenia regulaminu udzielania zamówień publicznych o wartości nieprzekraczającej kwoty 130.000,00 złotych

- Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet
- Przedstawienie rozwiązań zwiększających bezpieczeństw styku sieci lokalnej z siecią Internet

2.2. Testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji
- Analiza topologii sieci LAN
- Weryfikacja mechanizmów ochronnych w sieci
- Analiza komunikacji sieciowe
- Skanowanie portów TCP/UDP próba wykrycia usług sieciowych
- Skanowanie hostów aktywnych w sieci
- Exploitacja dostępnych urządzeń oraz usług w sieci LAN
- Przedstawienie rozwiązań zwiększających bezpieczeństw sieci LAN

3. Audyt ochrony danych zgodnie z przepisami RODO i UODO:
   3.1. Analiza zgodności dokumentacji ochrony danych osobowych
   3.2. Analiza upoważnień do przetwarzania danych osobowych
   3.3. Analiza umów powierzenia przetwarzania danych osobowych
   3.4. Analiza umów i porozumień dotyczących przekazywania danych osobowych
   3.5. Analiza wszystkich procesów przetwarzania danych
   3.6. Analiza rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania
   3.7. Ocena procesu zarządzania incydentami i reagowania na incydenty. Analiza informacji lub raportów dotyczących, incydentów naruszenia bezpieczeństwa danych
   3.8. Analiza konieczności dokonania oceny skutków dla planowanych sposobów przetwarzania danych
   3.9. Rozpoznanie roli i funkcji IODO
4. Analiza i szacowanie ryzyka w oparciu o normę PN-ISO/IEC 27005:2014
   4.1. Inwentaryzacja aktywów podlegających szacowaniu ryzyka,
   4.2. Określenie zagrożeń dla wyznaczonych aktywów,
   4.3. Określenie podatności dla wyznaczonych aktywów,
   4.4. Określenie prawdopodobieństw dla wyznaczonych aktywów,
   4.5. Oszacowanie ryzyka pod kątem skutków naruszenia bezpieczeństwa informacji.
5. Opracowanie dokumentacji Polityki bezpieczeństwa informacji, definiującej wymagania bezpieczeństwa i ochrony informacji wraz z Politykami bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji, w tym dla obszaru
   5.1. Teleinformatycznego
   5.2. Zabezpieczeń fizycznych
   5.3. Ciągłości działania
   5.4. Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji
   5.5. Procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z polityk bezpieczeństwa
6. Wyniki audytu:
   6.1. Raport z przeprowadzonego audyt zawierający ocenę stosowanych zabezpieczeń, analizę stanu bezpieczeństwa, wnioski, zalecenia i rekomendację dotyczące zakresu, metodyki i organizacji zabezpieczeń
   6.2. Rekomendacje dotyczące technicznych zabezpieczeń danych i informacji
   6.3. Raport z analizy ryzyka
   6.4. Dokumentacja SZB
   6.5. Wypełniony Arkusz do oceny JST (załącznik nr 8 Konkursu).

7. Wymogi
   7.1. Diagnoza cyberbezpieczeństwa (audyt) musi zostać przeprowadzony zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. 2017 poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI
   7.2. Diagnoza musi zostać wykonana zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronach Centrum Projektów Polska Cyfrowa [https://www.gov.pl/web/cppc/cyfrowa-gmina] - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8.
   7.3. Audyt musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane 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 oraz minimum 5 letnie doświadczenie. Wykaz certyfikatów wskazanych w w/w rozporządzeniu:
      7.3.1. Certified Internal Auditor (CIA)
      7.3.2. Certified Information System Auditor (CISA)
      7.3.3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób.
      7.3.4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób
      7.3.5. Certified Information Security Manager (CISM)
      7.3.6. Certified in Risk and Information Systems Control (CRISC)
      7.3.7. Certified in the Governance of Enterprise IT (CGEIT)
      7.3.8. Certified Information Systems Security Professional (CISSP)
      7.3.9. Systems Security Certified Practitioner (SSCP)
      7.3.10. Certified Reliability Professional
      7.3.11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.
   7.4. Wykonawca zrealizował przynajmniej 10 audytów bezpieczeństwa informacji w instytucjach publicznych w latach 2020 – 2022. Wykonawca, którego oferta zostanie uznana za najkorzystniejszą zobowiązany będzie do przedstawienia wykazu usług i referencji potwierdzających należyte wykonanie tych usług wraz z ofertą,
   7.5. Dysponuje w ramach umowy o pracę osobami zdolnymi zrealizować zamówienie:
      7.5.1. Trzech audytorów z wykształceniem wyższym z ochrony danych osobowych, w tym jeden z wyższym technicznym informatycznym
      7.5.2. Trzech audytorów wiodących ISO/IEC 27001:2013 ze zdanym egzaminem IRCA,
      7.5.3. Jeden audytor wiodący ISO/IEC 22301 ze zdanym egzaminem IRCA,
      7.5.4. Audytor posiadający zaświadczenie Certified Information Systems Security Officer (CISSO) lub równoważny,
      7.5.5. Audytor posiadający certyfikat Microsoft Certified Solutions Expert (MCSE) lub równoważny,

7.6. Prowadzi działalność w zakresie, którego dotyczy przedmiot zamówienia przez okres co najmniej 7 lat przed dniem złożenia oferty.
7.7. Posiada polisę ubezpieczeniową o wartości co najmniej 150 000 zł.
7.8. Posiada aktualne zaświadczenie o niezaleganiu ze składkami w ZUS oraz podatkami w US.
7.9. Nie jest dopuszczalne wykonywanie audytu przez podwykonawców.

Wykonawca, którego oferta zostanie uznana za najkorzystniejszą zobowiązany będzie do przedstawienia wymaganych certyfikatów i dokumentów.