Załącznik nr 3 do zapytania ofertowego

IOŚ.271.50.2022

# OPIS PRZEDMIOTU ZAMÓWIENIA

Poniżej zaprezentowane zostały minimalne wymagania Zamawiającego odnośnie wykonywanych przez Wykonawcę w ramach Zamówienia pn. **„Diagnoza cyberbezpieczeństwa oraz szkolenie administratora i pracowników Urzędu Gminy Gzy"** usług.

## Sporządzenie audytu cyberbezpieczeństwa

Przeprowadzenie audytu cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina" w Urzędzie Gminy Gzy (w dokumentacji projektu określanego jako „diagnoza cyberbezpieczeństwa") w zakresie oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji z obowiązującymi aktami prawnymi, w ty, w szczególności weryfikacji struktury organizacji oraz przepływu dokumentów elektronicznych, analizy zewnętrznej i wewnętrznej sieci komputerowej, analizy serwerów, testów dostępu do sieci wewnętrznej i zewnętrznej, analizy stacji roboczych, analizy kopii zapasowych, analizy poczty elektronicznej, analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli w Urzędzie, wraz z przygotowaniem raportu z audytu.
Audyt musi zostać przeprowadzony zgodnie z Ustawą z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 z późn. zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 z pózn. zm.).
Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 8 konkursu grantowego, załączony do niniejszego Zapytania ofertowego jako Załącznik nr 4.
Wykonawca zobowiązany jest do przedstawienia wyników audytu w formie papierowej oraz elektronicznej.

## Szkolenie administratora systemów IT Urzędu Gminy Gzy z zakresu cyberbezpieczeństwa

Szkolenie z zakresu cyberbezpieczeństwa dla administratora systemów IT ma na celu podniesienie kompetencji w obszarze zagrożeń teleinformatycznych, podniesienie poziomu bezpieczeństwa informacyjnego w Urzędzie, poznanie prawidłowej reakcji na cyberataki, podniesienie świadomości w zakresie potencjalnych cyberryzyk i incydentów oraz zdobycie umiejętności wykorzystania tej

wiedzy w praktyce. Szkolenie w swym zakresie winno obejmować co najmniej następujące zagadnienia:

1. Omówienie poprawnych zasad związanych z cyberbezpieczeństwem w Urzędzie, w szczególności wynikających z obowiązujących w tym zakresie aktów prawnych (Ustawa o krajowym systemie cyberbezpieczeństwa, Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności i inne).
2. Szczegółowe informacje związane z zagrożeniami w sieci, w szczególności: phishing, ransomware oraz malware i omówienie sposobów przeciwdziałania oraz zabezpieczenia się przed powyższym zagrożeniami.
3. Metody prawidłowej konfiguracji urządzeń sieciowych w celu zapewnienia bezpieczeństwa funkcjonowania sieci wewnętrznej Urzędu, w szczególności wykorzystania zapory sieciowej oraz backupu danych.

Wykonawca ma obowiązek przeprowadzenia szkolenia w formie teoretycznej oraz praktycznej, z uwzględnieniem zasobów sieciowych będących w posiadaniu Urzędu Gminy Gzy, w szczególności zapory sieciowej i systemu backupu danych.

Wykonawca w ramach usługi przeprowadzi szkolenie administratora systemów IT z Urzędu Gminy Gzy (1 osoba). Przed realizacją usługi przygotuje harmonogram szkolenia oraz jego program i dostarczy je w terminie nie później niż 7 dni przed planowanym dniem rozpoczęcia szkolenia do akceptacji przez Zamawiającego. Szkolenie odbyć się musi w formie stacjonarnej w siedzibie Zamawiającego.

Wykonawca przygotuje i zapewni uczestnikowi szkolenia najpóźniej w dniu szkolenia materiały szkoleniowe pozwalające na samodzielną edukację z zakresu tematyki szkolenia (np. opracowania, wydruki materiałów szkoleniowych). Dopuszczalne jest dostarczenie tych materiałów w formie elektronicznej np. plików w formacie PDF. Koszty związane z przygotowaniem i dostarczeniem materiałów szkoleniowych ponosi Wykonawca.

Wykonawca jest zobowiązany do zapewnienia uczestnikowi szkolenia możliwości konsultacji bezpośrednio po ukończeniu szkolenia, a także wskaże adres mailowy oraz kontakt telefoniczny w godzinach 8.00-15.00 w dni robocze, na który w ciągu 5 dni roboczych od ukończenia szkolenia uczestnik będzie mógł kierować pytania oraz udzieli na nie odpowiedzi w terminie nie późniejszym niż 10 dni roboczych od ukończenia szkolenia.

Szkolenie musi być certyfikowane. Wykonawca w ramach realizacji Zamówienia zapewni uczestnikowi szkolenia imienny certyfikat potwierdzający ukończenie szkolenia ze wskazaniem jego zakresu.

**<u>Szkolenie urzędników Urzędu Gminy Gzy z zakresu cyberbezpieczeństwa</u>**

Szkolenie z zakresu cyberbezpieczeństwa ma na celu podniesienie kompetencji kadry urzędniczej w obszarze zagrożeń teleinformatycznych, podniesienie poziomu bezpieczeństwa informacyjnego w Urzędzie, poznanie prawidłowej reakcji na cyberataki, podniesienie świadomości w zakresie potencjalnych cyberryzyk oraz incydentów, unikanie nieświadomego naruszenia bezpieczeństwa

informacji podczas pracy zdalnej, poznanie podstawowych zasad i dobrych praktyk wykorzystania technologii informatycznych oraz zdobycie umiejętności wykorzystania tej wiedzy w praktyce. Szkolenie w swym zakresie winno obejmować co najmniej następujące zagadnienia:

1. Omówienie poprawnych zasad związanych z cyberbezpieczeństwem w Urzędzie, w szczególności wynikających z obowiązujących w tym zakresie aktów prawnych (Ustawa o krajowym systemie cyberbezpieczeństwa, Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności i inne).
2. Szczegółowe informacje związane z zagrożeniami w sieci, w szczególności: phishing, ransomware oraz malware i omówienie sposobów przeciwdziałania oraz zabezpieczenia się przed powyższym zagrożeniami.

Wykonawca w ramach usługi przeprowadzi szkolenie dla 30 urzędników z Urzędu Gminy Gzy. Przed realizacją usługi przygotuje harmonogram szkolenia oraz jego program i dostarczy je w terminie nie później niż 7 dni przed planowanym dniem rozpoczęcia szkolenia do akceptacji przez Zamawiającego. Szkolenie odbyć się musi w formie stacjonarnej w siedzibie Zamawiającego. Zamawiający udostępni pomieszczenie umożliwiające przeprowadzenie szkolenia w grupach maksymalnie 10 osobowych.

Wykonawca przygotuje i zapewni wszystkim uczestnikom najpóźniej w dniu szkolenia materiały szkoleniowe pozwalające na samodzielną edukację z zakresu tematyki szkolenia (np. opracowania, wydruki materiałów szkoleniowych). Dopuszczalne jest dostarczenie tych materiałów w formie elektronicznej np. plików w formacie PDF. Koszty związane z przygotowaniem i dostarczeniem materiałów szkoleniowych ponosi Wykonawca.

Wykonawca jest zobowiązany do zapewnienia uczestnikom możliwości konsultacji bezpośrednio po ukończeniu szkolenia, a także wskaże adres mailowy na który w ciągu 7 dni od ukończenia szkolenia uczestnicy będą mogli kierować pytania oraz udzieli na nie odpowiedzi w terminie nie późniejszym niż 10 dni od ukończenia szkolenia.

Szkolenie musi być certyfikowane. Wykonawca w ramach realizacji Zamówienia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzające ukończenie szkolenia ze wskazaniem jego zakresu.

GMINA GZY
06-126 GZY
pow. pułtuski, woj. mazowieckie
NIP 568-15-45-506,REGON 130378114

WÓJT
Cezary Andrzej Wojciechowski

## OCENA ZGODNOŚCI Z KRI*/ UoKSC**

**Zasady oceny**

Każdemu z zagadnień (opisywanych wymagań), w polu oznaczonym na żółto, należy przypisać ocenę wg poniższej skali:

| | |
|---|---|
| 0 | Brak informacji o spełnieniu wymagania. |
| 1 | Zbieżność oświadczeń osób audytowanych. |
| 2 | Informacja udokumentowana. |

| Lp. | Opis wymagania | Podstawa | Audytowany | Dowody | Ustalenia | Ocena |
|---|---|---|---|---|---|---|
| 1 | Wyznaczenie osoby do kontaktu | Art. 21 UoKSC | | | | 1 |
| 2 | Przekazanie danych osoby wyznaczonej | Art. 22 ust. 1 pkt 5 UoKSC | | | | 0 |
| 3 | Zapewnienie zarządzania incydentem | Art. 22 ust. 1 pkt 1 UoKSC | | | | 0 |
| 4 | Zgłaszanie incydentu | Art. 22 ust. 1 pkt 2 UoKSC<br>Art. 23 UoKSC | | | | 0 |
| 5 | Zapewnienie obsługi incydentu | Art. 22 ust. 1 pkt 3 UoKSC | | | | 0 |
| 6 | Zapewnienie dostępu do wiedzy | Art. 22 ust. 1 pkt 4 UoKSC | | | | 0 |
| 7 | Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) | Par. 20 ust. 1 KRI | | | | 0 |
| 8 | Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) | Par. 20 ust. 1 KRI | | | | 0 |
| 9 | Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) | Par. 20 ust. 1 KRI | | | | 0 |
| 10 | Aktualizowanie regulacji wewnętrznych | Par. 20 ust. 2 pkt 1 KRI | | | | 0 |
| 11 | Inwentaryzacja sprzętu i oprogramowania | Par. 20 ust. 2 pkt 2 KRI | | | | 0 |
| 12 | Przeprowadzanie okresowych analiz ryzyka | Par. 20 ust. 2 pkt 3 KRI | | | | 0 |
| 13 | Postępowanie z ryzykiem | Par. 20 ust. 2 pkt 3 KRI | | | | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 14 | Zarządzanie uprawnieniami | Par. 20 ust. 2 pkt 4, 5 KRI | | | | 0 |
| 15 | Szkolenia i uświadamianie | Par. 20 ust. 2 pkt 6 KRI | | | | 0 |
| 16 | Monitorowanie dostępu do informacji | Par. 20 ust. 2 pkt 7 lit. a KRI | | | | 0 |
| 17 | Monitorowanie nieautoryzowanych zmian | Par. 20 ust. 2 pkt 7 lit. b KRI | | | | 0 |
| 18 | Zabezpieczenie nieautoryzowanego dostępu | Par. 20 ust. 2 pkt 7 lit. c KRI | | | | 0 |
| 19 | Ustanowienie zasad bezpiecznej pracy mobilnej | Par. 20 ust. 2 pkt 8 KRI | | | | 0 |
| 20 | Zabezpieczenie informacji przed nieuprawnionym ujawnieniem | Par. 20 ust. 2 pkt 9 KRI | | | | 0 |
| 21 | Zabezpieczenie informacji przed nieuprawnioną modyfikacją | Par. 20 ust. 2 pkt 9 KRI | | | | 0 |
| 22 | Zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem | Par. 20 ust. 2 pkt 9 KRI | | | | 0 |
| 23 | Zawieranie w umowach serwisowych zapisów o bezpieczeństwie | Par. 20 ust. 2 pkt 10 KRI | | | | 0 |
| 24 | Ustalenie zasad postępowania z informacjami w celu minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania | Par. 20 ust. 2 pkt 11 KRI | | | | 0 |
| 25 | Aktualizowanie oprogramowania | Par. 20 ust. 2 pkt 12 lit. a KRI | | | | 0 |
| 26 | Minimalizowanie ryzyka utraty informacji w wyniku awarii systemu | Par. 20 ust. 2 pkt 12 lit. b KRI | | | | 0 |
| 27 | Ochrona systemu przed błędami | Par. 20 ust. 2 pkt 12 lit. c KRI | | | | 0 |
| 28 | Stosowanie mechanizmów kryptograficznych w systemach | Par. 20 ust. 2 pkt 12 lit. d KRI | | | | 0 |
| 29 | Zapewnienie bezpieczeństwa plików systemowych | Par. 20 ust. 2 pkt 12 lit. e KRI | | | | 0 |
| 30 | Zarządzanie podatnościami systemów | Par. 20 ust. 2 pkt 12 lit. f, g KRI | | | | 0 |
| 31 | Kontrola zgodności systemów z regulacjami | Par. 20 ust. 2 pkt 12 lit. h KRI | | | | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 32 | Zapewnienie audytu bezpieczeństwa informacji, nie rzadziej niż raz na rok | Par. 20 ust. 2 pkt 14 KRI | | | | 0 |

*Rozporządzenie 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 (Dz.U. z 2017 r. poz. 2247, t.j.)

**Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.).