Załącznik nr 3 do zapytania ofertowego

w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotyczące realizacji projektu grantowego „Cyfrowa Gmina"

OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ II

PRZEPROWADZENIE AUDYTU CYBERBEZPIECZEŃSTWA GMINY DRAWNO

W ramach realizacji przedmiotu zamówienia Wykonawca będzie zobowiązany do dokonania oceny zgodności funkcjonalnych zasad i procedur dotyczących zarządzania bezpieczeństwem informacji w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi do przeprowadzenia kompleksowego audytu informacji w zakresie ustawowych obszarów działalności podmiotu oraz opracowania dokumentacji po audytowej – raportu z wytycznymi do doskonalenia i rekomendacji.

1. Diagnoza cyberbezpieczeństwa w Urzędzie Gminy Drawno musi zostać przeprowadzona 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.), w tym opracowanie raportu zawierającego wnioski i rekomendacje.
2. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronach Centrum Projektów Polska Cyfrowe (https://www.gov.pl/web/cppc/cyfrowa-gmina) – Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa – załącznik nr 8.
3. Audyt musi być 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. Wykaz wskazanych w w/w rozporządzeniu:
   a) Certified Internal Auditor (CIA)
   b) Certified Information System Auditor (CISA)
   c) 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

d) 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
e) Certified Information Security Manager (CISM)
f) Certified in Risk and Information Systems Control (CRISC)
g) Certified in the Governance of Enterprise IT (CGEIT)
h) Certified Information Systems Security Professional (CISSP)
i) Systems Security Certified Practitioner (SSCP)
j) Certified Reliability Professional
k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

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

Załączniki do opisu diagnozy cyberbezpieczeństwa:

1. Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa
2. Rozporządzenie Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu

DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 18 października 2018 r.

Poz. 1999

ROZPORZĄDZENIE
MINISTRA CYFRYZACJI[1)]

z dnia 12 października 2018 r.

w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu

Na podstawie art. 15 ust. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) zarządza się, co następuje:

§ 1. Rozporządzenie określa wykaz certyfikatów uprawniających do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stanowiący załącznik do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Minister Cyfryzacji: *M. Zagórski*

[1)] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 20 kwietnia 2018 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 761).

Załącznik do rozporządzenia Ministra Cyfryzacji
z dnia 12 października 2018 r. (poz. 1999)

WYKAZ CERTYFIKATÓW UPRAWNIAJĄCYCH DO PRZEPROWADZANIA AUDYTU

1. Certified Internal Auditor (CIA);
2. Certified Information System Auditor (CISA);
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;
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;
5. Certified Information Security Manager (CISM);
6. Certified in Risk and Information Systems Control (CRISC);
7. Certified in the Governance of Enterprise IT (CGEIT);
8. Certified Information Systems Security Professional (CISSP);
9. Systems Security Certified Practitioner (SSCP);
10. Certified Reliability Professional;
11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

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 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.).