AUDYT CYBERBEZPIECZEŃSTWA ZGODNIE Z ZAKRESEM WSKAZANYM W DOKUMENTACJI KONKURSOWEJ PROJEKTU CYFROWA GMINA

https://www.gov.pl/web/cppc/cyfrowa-gmina

1. Przeprowadzenie **audytu cyberbezpieczeństwa w siedzibie Zamawiającego** zgodnie z **zakresem wskazanym w załączniku nr 8** do *„Regulaminu Konkursu Grantowego Cyfrowa Gmina Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia Program Operacyjny Polska Cyfrowa”*. W szczególności:

   - ocena zgodności z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369);
   - ocena zgodności z 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 (Dz.U. z 2017 r. poz. 2247 t.j.);
   - ocena wybranych aspektów bezpieczeństwa systemów informatycznych.

   Szczegółowy zakres audytu zamieszczono w załączniku numer 1 do zapytania.

   Czas trwania audytu w siedzibie Zamawiającego nie krócej niż 2 dni robocze. Zamawiający nie udostępnia dokumentacji wymaganej do przeprowadzenia audytu poza siedzibę Jednostki (audyt „na miejscu” u Zamawiającego).

2. **Przekazanie dla Zamawiającego sprawozdania z audytu cyberbezpieczeństwa** opisującego kryteria dotyczące audytu, ustalenia wynikające z audytu oraz wnioski i zalecenia wypływające z audytu.

3. **Przekazanie dla zamawiającego uzupełnionego załącznika numer 8** do Regulaminu Konkursu Grantowego Cyfrowa Gmina – załącznik *„Arkusz_do_oceny_JST_w_konkursie_Cyfrowa_Gmina”*.

Audytor jest zobowiązany posiadać uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001999/O/D20181999.pdf Zamawiający zastrzega możliwość weryfikacji uprawnień audytora (ważności uprawnień, akredytacja jednostki wydającej uprawnienia).

Załącznik 1. Szczegółowy zakres audytu.

I. Ocena zgodności Jednostki z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369) dalej UoKSC.

Lp.	Opis wymagania.	Podstawa prawna.
1	Wyznaczenie osoby do kontaktu	Art. 21 UoKSC
2	Przekazanie danych osoby wyznaczonej	Art. 22 ust. 1 pkt 5 UoKSC
3	Zapewnienie zarządzania incydentem	Art. 22 ust. 1 pkt 1 UoKSC
4	Zgłaszanie incydentu	Art. 22 ust. 1 pkt 2 UoKSC Art. 23 UoKSC
5	Zapewnienie obsługi incydentu	Art. 22 ust. 1 pkt 3 UoKSC
6	Zapewnienie dostępu do wiedzy	Art. 22 ust. 1 pkt 4 UoKSC

II. Ocena wybranych aspektów bezpieczeństwa systemów informatycznych.

Lp.	Zagadnienie
1	**Dokumentacja potwierdzająca wykonane działania wskazanego w ustawie o krajowym systemie cyberbezpieczeństwa (UoKSC)**
1.1	Czy zostały zidentyfikowane usługi publiczne, których świadczenie zależy od bezpieczeństwa systemów informacyjnych?
1.2	Czy zostały wskazane osoby (podmioty) odpowiedzialne za zarządzanie incydentami?
1.3	Czy podmiot publiczny realizuje zadania publikowania informacji pozwalających na zrozumienie zagrożeń cyberbezpieczeństwa oraz możliwych, skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, tj. zadań zawartych w art. 22 ust. 1 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.)?
1.4	Czy została wyznaczona i zgłoszona do właściwego CSIRT, osoba kontaktowa, o której mowa w art. 21 oraz art. 22 ust. 1 pkt 5 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.)?
2	**Opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne**
2.1	Czy wszystkie elementy składowe systemu informatycznego zostały zinwentaryzowane?
2.2	Czy dla każdego systemu informatycznego utrzymywana jest aktualna lista osób odpowiedzialnych za jego bezpieczną eksploatację?
3	**Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne**
3.1	Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne?
3.2	Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń?
3.3	Czy istnieje dokumentacja architektury sieci?
3.4	Czy istnieje baza danych konfiguracji urządzeń aktywnych?
3.5	Czy istnieje dokumentacja zmian w systemach informacyjnych?
3.6	Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym?
3.7	Czy są dostępne umowy z dostawcami (wsparcie techniczne)?
3.8	Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego?
3.9	Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego?
3.10	Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych?
3.11	Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego?
4	**Dokumentacja procesu zarządzania incydentami**
4.1	Czy wdrożone jest monitorowanie i wykrywanie incydentów? Kto za nie odpowiada? (stanowiska, funkcje itp. - bez danych osobowych)
4.2	Czy istnieje procedura informowania o wykrytych incydentach?
4.3	Czy istnieją procedury reagowania na incydenty?

5	**Aspekty techniczne do weryfikacji**
5.1	Wyniki audytu serwisów WWW z uwzględnieniem: - wersji serwera HTTP; - wersji systemu CMS (o ile występuje); - bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.); - dostępności kompetentnego personelu do utrzymania serwisów.
5.2	Wyniki audytu serwisów pocztowych z uwzględnieniem: - poprawności wdrożenia mechanizmów SPF, DKIM i DMARC; - poprawności i bezpieczeństwa wdrożenia mechanizmów TLS; - dostępności kompetentnego personelu do utrzymania serwisów.
5.3	Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem: - wdrożenia systemów ochrony przed kodem szkodliwym w sposób zapewniający ich automatyczną aktualizację; - stosowania mechanizmów segmentacji sieci; - izolacji urządzeń końcowych użytkowników; - procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji; - monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa; - dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej.
5.4	Wyniki audytu połączenia z siecią Internet z uwzględnieniem: - monitorowania ruchu wchodzącego i wychodzącego; - stosowanych zabezpieczeń przed atakami DDoS; - stosowanych zabezpieczeń przed wyciekiem informacji (DLP); - stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.); - dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet.
6	**Aspekty organizacyjne do weryfikacji**
6.1	Wyniki audytu organizacji zarządzania bezpieczeństwem teleinformatycznym z uwzględnieniem: - regularnego identyfikowania znanych podatności w eksploatowanych systemach IT; - terminowego wprowadzania danych do systemów zarządzania tożsamością i uprawnieniami użytkowników; - prowadzenia okresowego przeglądu uprawnień użytkowników; - prowadzenia okresowych szkoleń użytkowników podnoszących ich świadomość zagrożeń.
6.2	Wyniki audytu procesów planowania z uwzględnieniem: - posiadania planów przywracania usług IT na wypadek awarii; - prowadzenia przeglądów oraz doskonalenia planów przywracania usług IT; - cyklu życia systemów IT i eksploatacji produktów nieposiadających wsparcia producenta.

III. Ocena zgodności Jednostki z 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 (Dz.U. z 2017 r. poz. 2247 t.j.) dalej KRI.

Lp.	Opis wymagania	Podstawa prawna.
1	Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI
2	Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI

3	Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI
4	Aktualizowanie regulacji wewnętrznych	Par. 20 ust. 2 pkt 1 KRI
5	Inwentaryzacja sprzętu i oprogramowania	Par. 20 ust. 2 pkt 2 KRI
6	Przeprowadzanie okresowych analiz ryzyka	Par. 20 ust. 2 pkt 3 KRI
7	Postępowanie z ryzykiem	Par. 20 ust. 2 pkt 3 KRI
8	Zarządzanie uprawnieniami	Par. 20 ust. 2 pkt 4, 5 KRI
9	Szkolenia i uświadamianie	Par. 20 ust. 2 pkt 6 KRI
10	Monitorowanie dostępu do informacji	Par. 20 ust. 2 pkt 7 lit. a KRI
11	Monitorowanie nieautoryzowanych zmian	Par. 20 ust. 2 pkt 7 lit. b KRI
12	Zabezpieczenie nieautoryzowanego dostępu	Par. 20 ust. 2 pkt 7 lit. c KRI
13	Ustanowienie zasad bezpiecznej pracy mobilnej	Par. 20 ust. 2 pkt 8 KRI
14	Zabezpieczenie informacji przed nieuprawnionym ujawnieniem	Par. 20 ust. 2 pkt 9 KRI
15	Zabezpieczenie informacji przed nieuprawnioną modyfikacją	Par. 20 ust. 2 pkt 9 KRI
16	Zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem	Par. 20 ust. 2 pkt 9 KRI
17	Zawieranie w umowach serwisowych zapisów o bezpieczeństwie	Par. 20 ust. 2 pkt 10 KRI
18	Ustalenie zasad postępowania z informacjami w celu minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania	Par. 20 ust. 2 pkt 11 KRI
19	Aktualizowanie oprogramowania	Par. 20 ust. 2 pkt 12 lit. a KRI
20	Minimalizowanie ryzyka utraty informacji w wyniku awarii systemu	Par. 20 ust. 2 pkt 12 lit. b KRI
21	Ochrona systemu przed błędami	Par. 20 ust. 2 pkt 12 lit. c KRI
22	Stosowanie mechanizmów kryptograficznych w systemach	Par. 20 ust. 2 pkt 12 lit. d KRI
23	Zapewnienie bezpieczeństwa plików systemowych	Par. 20 ust. 2 pkt 12 lit. e KRI
24	Zarządzanie podatnościami systemów	Par. 20 ust. 2 pkt 12 lit. f, g KRI
25	Kontrola zgodności systemów z regulacjami	Par. 20 ust. 2 pkt 12 lit. h KRI
26	Zapewnienie audytu bezpieczeństwa informacji, nie rzadziej niż raz na rok	Par. 20 ust. 2 pkt 14 KRI