Sfinansowano w ramach reakcji Unii na pandemię COVID-19

NASK

Diagnoza Cyberbezpieczeństwa – zalecenia dotyczące zasad wypełniania i wysyłania do NASK dokumentów w ramach konkursu grantowego „Cyfrowy Powiat"

Wprowadzenie

Szanowni Państwo,

od jakości i kompletności danych przekazanych w diagnozach cyberbezpieczeństwa będą zależeć wyniki przeprowadzanych badań i możliwości wnioskowania na ich podstawie. Rezultaty badań zostaną opracowane w formie zbiorczych zestawień i umieszczone w raporcie przeznaczonym dla Departamentu Cyberbezpieczeństwa KPRM. Dane, przed ich przetworzeniem, zostaną zanonimizowane, aby nie można ich było odnieść do konkretnego Grantobiorcy.

Podstawa prawna

Zgodnie z §4 pkt 8 Regulaminu Konkursu Grantowego Cyfrowy Powiat obligatoryjna jest realizacja zadania związanego z przeprowadzeniem diagnozy cyberbezpieczeństwa. Diagnoza cyberbezpieczeństwa powinna zostać przeprowadzona zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do ww. Regulaminu.

Załącznik nr 8 - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa

Po przeprowadzeniu diagnozy Grantobiorca zobligowany jest przekazać do NASK wypełniony formularz diagnozy, przeprowadzonej przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. Diagnozę należy przesłać za pomocą elektronicznej skrzynki podawczej ePUAP do NASK na adres skrzynki: **/NASK-Instytut/SkrytkaESP** (akronim/temat: cyfrowy.powiat.diagnoza.cyber).

Zalecenia dotyczące wysyłki dokumentów do NASK

I. Dokumenty przekazywane do NASK-PIB:

1. Pismo przewodnie zawierające:
   - dane Grantobiorcy: nazwa, adres, NIP, Regon, Teryt;
   - dane osoby kontaktowej: imię, nazwisko, telefon, mail;
   - krótki opis przedmiotu sprawy, np. przekazanie diagnozy cyberbezpieczeństwa w ramach konkursu grantowego „Cyfrowy Powiat".
2. Załącznik nr 8 do Regulaminu w formacie **.xlsx** lub **.xls** (edytowalny plik Excel).
3. Załącznik nr 8 do Regulaminu w formacie **.pdf** (zaleca się, aby wersja PDF była podpisana przez audytora wykonującego diagnozę).

II. Adres skrzynki podawczej:

Dokumenty należy przesłać za pomocą elektronicznej skrzynki podawczej ePUAP do NASK – Państwowy Instytut Badawczy na adres skrzynki:

/NASK-Instytut/SkrytkaESP
(akronim/temat: cyfrowy.powiat.diagnoza.cyber)

Uwaga:
Wszystkie znaki w adresie skrzynki podawczej muszą być zgodne z podanym wzorem, w tym istotna jest pisownia wielką lub małą literą. W adresie skrzynki podawczej znajduje się łącznik (dywiz), wprowadzany jest on poprzez wciśnięcie klawisza [minus].

UPP:
Każda poprawna wysyłka jest automatycznie potwierdzana Urzędowym Poświadczeniem Przedłożenia.

Zalecenia dotyczące sposobu wypełniania załącznika nr 8

W załączniku nr 8 znajdują się 3 arkusze: <<KRI>>, <<CERT>> oraz <<Skala>>.
Ocenie podlegają 2 arkusze: <<KRI>> oraz <<CERT>>.

I. W arkuszu KRI należy:

1. Wypełnić wszystkie pola (ocenić 32 wymagania).
   Pola do wypełnienia mają biały lub żółty kolor.

2. Oceny opisowe (tekstowe) należy wpisać w puste pola zaznaczone na biało (kol. od E do G).

3. W kol. H w polach zaznaczonych na żółto (pola wyboru) należy dokonać oceny wg podanej w arkuszu skali, tj. od 0 do 2.
   Domyślna wartość to „0".

ARKUSZ KRI (fragment)

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				0
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

II. W arkuszu CERT należy:

1. Wypełnić wszystkie pola. Pola do wypełnienia mają biały lub żółty kolor.

2. Oceny opisowe (tekstowe) należy wpisać w puste pola zaznaczone na biało (kol. D).

3. W kol. E należy dokonać oceny TYLKO w polach zaznaczonych na żółto (pola wyboru) wg podanej w arkuszu skali, tj. od 0 do 4. Domyślna wartość to „0".

ARKUSZ CERT (fragment)

A	B	C	D	E	F
		OCENA WYBRANYCH ASPEKTÓW BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH			
	Zasady oceny				
	Każdemu z zagadnień, w polu oznaczonym na żółto, należy przypisać ocenę wg poniższej skali:				
	0	Całkowity brak realizacji wymagania. Brak świadomości wymogu.			
	1	Wymaganie spełnione w małym stopniu. Świadomość istnienia wymagania.			
	2	Częściowa realizacja wymagania.			
	3	Drobne niedociągnięcia, niewpływające na bezpieczeństwo IT.			
	4	Pełna zgodność z wymaganiami.			
	Lp.	Zagadnienie	Ustalenia	Ocena	
	1	**Dokumentacja potwierdzająca wykonane działania wskazanego w ustawie o krajowym systemie cyberbezpieczeństwa***		0	
	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**		0	
	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?			

Zalecenia dotyczące sposobu wypełniania pól opisowych (tekstowych) w arkuszach KRI oraz CERT

1. Należy wypełnić wszystkie wymagane pola.
2. Opisy powinny być spójne z dokonaną oceną.
3. Stosować jednoznaczne zapisy, wykorzystywać terminologię obowiązującą w ramach danego zagadnienia.
4. Nie należy stosować odsyłaczy do innych wierszy, takich jak: j.w., poniżej lub odwołań do opisów zawartych w innych polach (np. wpis w pkt 5 tak jak w pkt 3). Dane zawarte w konkretnym polu będą podlegały przetwarzaniu bez odwoływania się do danych w innych polach.
5. Nie należy wprowadzać hasła uniemożliwiającego otwarcie pliku ani też nie należy stosować haseł ograniczających modyfikację arkuszy.
6. Nie należy zmieniać struktury i szaty graficznej arkuszy, np. dodawanie, usuwanie wierszy, kolumn, dodatkowe dzielenie lub łączenie pól.

Kontakt w sprawie sposobu przekazywania dokumentów związanych z diagnozą cyberbezpieczeństwa

NASK – Państwowy Instytut Badawczy

ul. Kolska 12, 01-045 Warszawa

- **Recepcja NASK**
  tel.: 22 380 82 00
- **Zespół Zarządzania Wiedzą i Raportowania**
  Pani Justyna Chodkowska
  tel.: +48 882 436 231
  e-mail: justyna.chodkowska@nask.pl