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.



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**

1. **Dokumenty przekazywane do NASK-PIB:**
2. 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”.
1. Załącznik nr 8 do Regulaminu w formacie **.xlsx** lub **.xls**
(edytowalny plik Excel).
2. Załącznik nr 8 do Regulaminu w formacie **.pdf**

(zaleca się, aby wersja PDF była podpisana przez audytora
wykonującego diagnozę).

1. **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>>.

1. **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)



1. **W arkuszu CERT należy:**
2. Wypełnić wszystkie pola. Pola do wypełnienia mają biały lub żółty kolor.
3. Oceny opisowe (tekstowe) należy wpisać w puste pola zaznaczone na biało (kol. D).
4. 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)



 **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