NASK | Cyberbezpieczny Samorząd

Cyberbezpieczny Samorząd

Fundusze Europejskie na Rozwój Cyfrowy

Fundusze Europejskie na Rozwój Cyfrowy

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

AGENDA PREZENTACJI

NASK

1. Wprowadzenie
   - Wyniki kontroli NIK
   - Diagnoza Cyberbezpieczeństwa
   - Sankcje - przykłady
2. Cyberbezpieczny Samorząd
   - O projekcie
   - Dokumentacja konkursu grantowego
3. Planowanie rozwoju JST w obszarze cyberbezpieczeństwa
4. Poradnik
5. Katalog kosztów kwalifikowanych
6. Lokalny system informatyczny (LSI)
7. Pytania i odpowiedzi

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

WYNIKI KONTROLI NIK

„Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

WYNIKI KONTROLI NIK

„Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”

NASK

Pytanie definiujące cel główny kontroli

Czy przyjęte i wdrożone rozwiązania organizacyjne i techniczne zapewniają bezpieczeństwo przetwarzania informacji w urzędzie?

Jednostki kontrolowane

Kontrolą objęto 23 jednostki: dziewięć starostw powiatowych oraz 14 urzędów miast/miast i gmin/gmin z obszaru pięciu województw.

Okres objęty kontrolą

Od 1 czerwca 2017 r. do dnia zakończenia kontroli w 2018 r.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

WYNIKI KONTROLI NIK

Ocena ogólna

NIK **negatywnie oceniła wykonywanie przez blisko 70% skontrolowanych urzędów** jednostek samorządu terytorialnego zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji w okresie objętym kontrolą.

Brak systemowego podejścia do zapewnienia bezpieczeństwa informacji

- W 61% skontrolowanych urzędów brak było systemowego podejścia do zapewnienia bezpieczeństwa informacji.
- W 74% badanych urzędów brak było pełnej i aktualnej informacji o posiadanych zasobach informatycznych służących do przetwarzania danych.
- W 26% urzędów stwierdzono niedostosowanie uregulowań wewnętrznych w zakresie ochrony danych osobowych do przepisów RODO.

Brak analiz ryzyka i nieprowadzenie audytów bezpieczeństwa informacji

- 48% jednostek nie dokonywano analiz ryzyka,
- a w 70% nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji.

Nieprzestrzeganie ustanowionych wymogów w zakresie bezpieczeństwa informacji

- W ponad 80% skontrolowanych urzędów wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych. W zakresie uzyskiwania dostępu do systemów informatycznych,
- w ponad połowie kontrolowanych urzędów (57%) ustanowione zasady nie były przestrzegane.
- W 56% jednostek wykorzystywano komputery z zainstalowanym systemem operacyjnym bez wsparcia producenta,
- a w 48% urzędów stwierdzono nieprawidłowości w zakresie tworzenia, przechowywania oraz weryfikacji kopii zapasowych danych.

Wdrażanie RODO a zapewnienie bezpieczeństwa informacji

Wyniki kontroli NIK wskazują, że o ile w urzędach j.s.t. w większości podjęto działania w celu dostosowania do RODO, to w dalszym ciągu często nie są przestrzegane wymogi dotyczące bezpieczeństwa informacji wynikające z obowiązującego od 2012 r. rozporządzenia KRI. W opinii NIK, nie jest możliwe zapewnienie wysokiego poziomu ochrony danych osobowych bez zachowania właściwego bezpieczeństwa informacji.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

badanie w ramach konkursów Cyfrowa Gmina/Powiat/Województwo

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Opracowanie, ustanowienie i wdrożenie SZBI

- 63% urzędów posiadało wdrożony zarządzeniem SZBI
  - Z czego tylko 40% podmiotów wykonuje jego okresowy przegląd
- 19% urzędów było w trakcie na różnym poziomie zaawansowania
- 18% nie podeszło do opracowania, ustanowienia i wdrożenia SZBI

W większości urzędów funkcjonują polityki w zakresie ochrony danych osobowych z elementami bezpieczeństwa informacji. Nie były one uznane za systemowe podejście do budowania i wdrożenia SZBI.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Przeprowadzanie okresowych analiz ryzyka

- 53% urzędów przeprowadza regularną analizę ryzyka
- 22% urzędów przeprowadza nieregularną lub w ograniczonym zakresie (np. tylko w odniesieniu do danych osobowych) analizę ryzyka
- 25% nie przedstawiło dowodów na przeprowadzenie analizy ryzyka

Ze względu na różnice w ocenie audytorów, wskaźnik 53% jest zawyżony, część audytujących uznawała analizy w zakresie DO za wystarczające. Podobnie zbyt dawne analizy ryzyka były klasyfikowane jako brak zwiększając odsetek czerwony.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Inwentaryzacja sprzętu i oprogramowania

- 63% urzędów przeprowadza regularną inwentaryzację/utrzymuje aktualny spis
- 22% urzędów wykorzystuje spisy środków trwałych i WNP lub przeprowadza inwentaryzację (utrzymanie wykazu) w sposób nieregularny
- 15% nie prowadzi własnych spisów i nie korzysta ze spisów księgowych

Ze względu na różnice w ocenie audytorów, wskaźnik 63% jest zawyżony, część audytujących uznawała spisy księgowe jako spełnienie wymagania. Jedynie 24% podmiotów przeprowadza inwentaryzację automatycznie, za pomocą dedykowanych narzędzi.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Szkolenia i uświadamianie

- **57% urzędów wskazało że szkoli i uświadamia, ale:**
  - Często są to tylko szkolenia w zakresie ochrony danych osobowych.
  - Często są to tylko szkolenia wprowadzające dla nowych pracowników.
  - Wiele urzędów ogranicza się do publikowania informacji w intranecie.

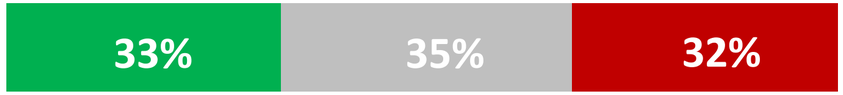
Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wyniki dla 2285 gmin (wybrane aspekty)

NASK

Zarządzanie podatnościami systemów



- **33% urzędów prowadzi zarządzanie podatnościami systemów, ale**
  - jedynie 8% podmiotów, stosując albo dedykowany skaner podatności (1% podmiotów) albo rozszerzoną funkcjonalność oprogramowania antywirusowego (7% podmiotów),
  - dbanie o aktualizacje i posiadanie wsparcia producenta nie wyczerpuje zagadnienia.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wnioski ogólne

NASK

Diagnoza Cyberbezpieczeństwa przyniosła wiele dobrego

- W wielu przypadkach pokazała problemy (bardziej od strony zgodności z prawem) zapewnienia bezpieczeństwa informacji.
- Otworzyła drzwi gabinetów włodarzy dla specjalistów od IT/Sec, dopuściła ich do planowania budżetów.

Diagnoza Cyberbezpieczeństwa uwidoczniła też poważne problemy

- Zapewnienie odporności na zagrożenia w cyberprzestrzeni jest zadaniem przekraczającym możliwości samodzielnej realizacji przez większość podmiotów JST (gmin).
- Podmioty nie posiadają kompetencji do zarządzania bezpieczeństwem, np. do przeprowadzania analiz ryzyka.
- Systematyczne zarządzanie bezpieczeństwem IT jest kosztowne, szczególnie, że do większości działań JST musi skorzystać z usług zewnętrznych.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

DIAGNOZA CYBERBEZPIECZEŃSTWA W JST

Wnioski ogólne – główne wyzwania

NASK

TECHNICZNE

- identyfikacja co i dlaczego chronimy?
- dobór klas rozwiązań
- zapewnienie ciągłości monitorowania
- utrzymanie zdolności do szybkiej reakcji

ORGANIZACYJNE

- wsparcie kierownictwa
- przygotowanie jednostki
- dyscyplina i higiena
- sprawność operacyjna

KOMPETENCYJNE

- budowanie świadomości
- kompetencje specjalistyczne
- weryfikowanie odporności

Jak zbudować System?

który chroni to co trzeba tak jak trzeba → który jest trwały i nie tylko na papierze → który dba o każde ogniwo

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

SANKCJE - PRZYKŁADY

SANKCJE - PRZYKŁADY

Wybrane kary nałożone przez Prezesa Urzędu Ochrony Danych

NASK

Podmiot	Wysokośc kary	Podstawa prawna	Data decyzji
Burmistrz Aleksandrowa Kujawskiego	9.380 euro	Art. 28 RODO	18.10.2019
Geodeta Generalny Polski	22.700 euro	Art. 5 RODO, Art. 6 RODO	31.08.2020
Prezes Sądu Rejonowego w Zgierzu	2.200 euro	Art. 5 (1) f) RODO, Art. 25 (1) RODO, Art. 32 (1) b), d), (2) RODO	13.08.2021
Główny Geodeta Kraju	12.450 euro	Art. 33 (1) RODO, Art. 34 (1) RODO	06.07.2022

stwierdzając naruszenie przez Burmistrza Miasta Z. (Urząd Miasta Z., ul. [...]), art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35), dalej jako rozporządzenie 2016/679, polegające na doborze nieskutecznych zabezpieczeń systemu informatycznego wykorzystywanego do przetwarzania danych osobowych oraz braku odpowiedniego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych objętych naruszeniem, w szczególności w zakresie podatności, błędów oraz ich możliwych skutków dla tych systemów oraz podjętych działań minimalizujących ryzyko ich wystąpienia:

stwierdzając naruszenie przez Burmistrza Miasta i Gminy W. (Urząd Miasta i Gminy W., ul. [...]) przepisów art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35), dalej jako rozporządzenie 2016/679, polegające na niezastosowaniu przez Burmistrza Miasta i Gminy W. odpowiednich środków organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych, co skutkowało nieuprawnionym wykonaniem kopii danych osobowych z komputera służbowego na przenośny nośnik pamięci przez pracownika Urzędu Miasta i Gminy W., nakłada na Burmistrza Miasta i Gminy W. (Urząd Miasta i Gminy W., ul. [...]) za naruszenie przepisów art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679 administracyjną karę pieniężną w kwocie 10 000 złotych (słownie: dziesięć tysięcy złotych).

▪ ▪ ▪

Źródło: na podstawie zestawienia w https://www.enforcementtracker.com

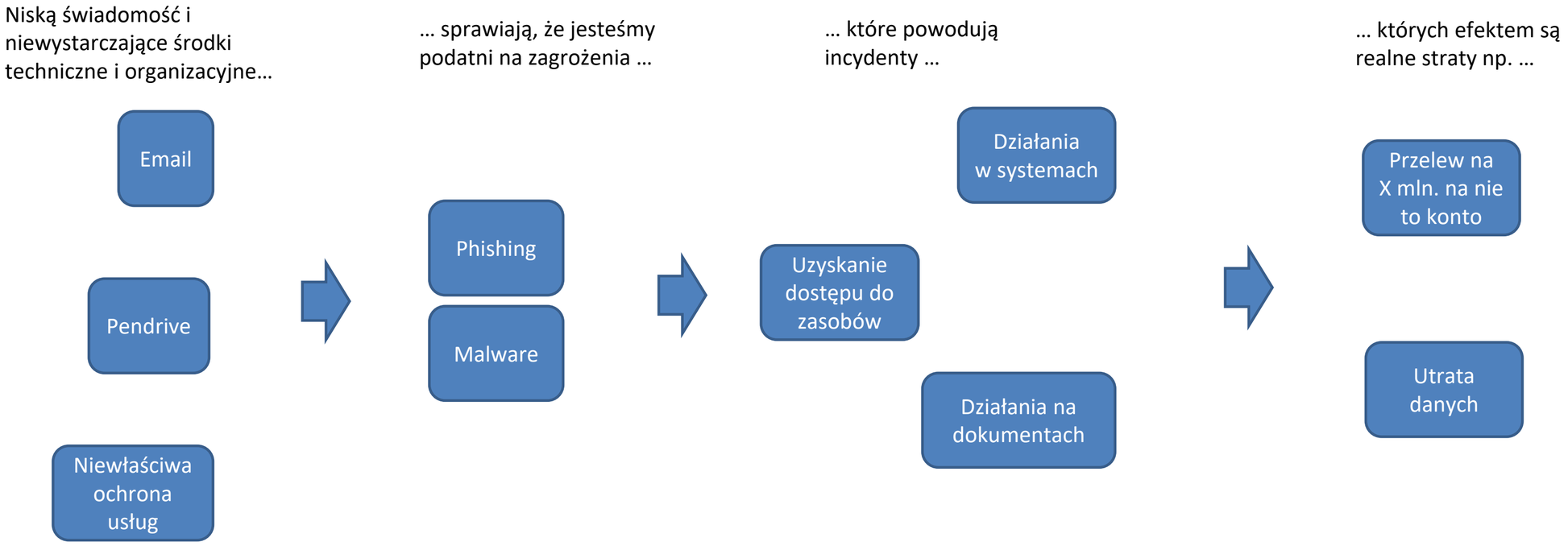
Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

SANKCJE - PRZYKŁADY

A co z KRI i uoKSC?

NASK

„Nie ma kar to nie robimy mamy ważniejsze wydatki”, tylko że:



Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

SANKCJE - PRZYKŁADY

A co z KRI i uoKSC?

NASK

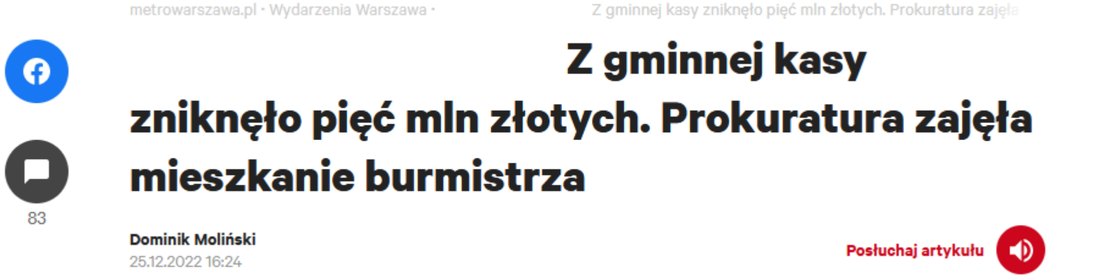
„Nie ma kar to nie robimy mamy ważniejsze wydatki”, tylko że:

*„Wobec burmistrza (…) sformułowano zarzut popełnienia przestępstwa polegającego na **nieumyślnym niedopełnieniu ciążących na nim obowiązków** i w związku z tym wyrządzenia szkody w obrocie w wielkich rozmiarach, to jest przestępstwa zagrożonego karą pozbawienia wolności do lat trzech”*

Na podstawie art. 296. KK

*„Burmistrz nie przyznał się do winy. Według prokuratury nie było konieczne zatrzymywanie go, podjęto jednak inne działanie. - Na poczet grożących podejrzanemu - w przypadku uznania go winnym oraz skazania - kary grzywny, orzeczenia obowiązku naprawienia szkody oraz zasądzenia obowiązku zapłaty kosztów sądowych w postępowaniu karnym, **dokonano zajęcia nieruchomości w postaci mieszkania stanowiącej własność podejrzanego**, wchodzącą w skład wspólności ustawowej majątkowej małżeńskiej, poprzez ustanowienie hipoteki przymusowej do kwoty łącznie pięciu milionów i dwudziestu tysięcy złotych.”*

Na podstawie art. 291. KPK



metrowarszawa.pl · Wydarzenia Warszawa · Z gminnej kasy zniknęło pięć mln złotych. Prokuratura zajęła

83

Z gminnej kasy zniknęło pięć mln złotych. Prokuratura zajęła mieszkanie burmistrza

Dominik Moliński
25.12.2022 16:24

Posłuchaj artykułu

Oszukana gmina straciła pięć milionów złotych. Prokuratura zajęła mieszkanie burmistrza

Podobnymi, również kosztownymi atakami padły samorządy miast w (…) i (…). W ich przypadku cyberprzestępcy dokonali **ataku na serwer VoIP** służący do nawiązywania połączeń telefonicznych z wykorzystaniem sieci internetowej. W przypadku (…) hakerzy wykonali prawie 900 połączeń do Zimbabwe, „naciągając” miasto na rachunek w wysokości 49 tys. zł, a (…) na 19,5 tys. zł poprzez telefony do sieci komórkowej w Austrii. (prawo.pl)

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie

NASK

„Cyberbezpieczny Samorząd” to projekt Ministerstwa Cyfryzacji finansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (w skrócie FERC) w ramach Działania 2.2.

2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa

Interwencja obejmie inwestycje zwiększające poziom bezpieczeństwa informacji poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotów mających kluczowe znaczenie dla gospodarki.

Celem projektu jest **zwiększenie bezpieczeństwa informacji w administracji samorządowej** poprzez wzmacnianie odporności oraz zdolności do **skutecznego zapobiegania i reagowania na incydenty.**

Sposób realizacji projektu

Projekt realizowany jest poprzez uruchomienie konkursu grantowego adresowanego jednostkom samorządu terytorialnego na poziomie gminy, powiatu, samorządu województwa. W ramach konkursu przyznane są granty na zakup usług i środków technicznych służących zwiększeniu poziomu cyberbezpieczeństwa jednostek samorządowych w obszarach: organizacji, kompetencji i technologii.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie

NASK

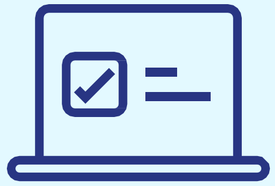
Zakłada się, że realizacja projektu przyczyni się do:

- wdrożenia lub aktualizacji w JST polityk bezpieczeństwa informacji (SZBI)
- wdrożenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie
- wdrożenia w JST mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni
- podniesienia poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie
- przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie



Organizatorem projektu grantowego jest Centrum Projektów Polska Cyfrowa (CPPC) realizująca projekt w Partnerstwie z Naukową i Akademicką Siecią Komputerową - Państwowym Instytutem Badawczym (NASK-PIB).

Nabór wniosków grantowych realizowany jest w ramach otwartego naboru grantowego na postawie regulaminu dostępnego na stronie: **https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad**

Składanie wniosków grantowych w projekcie „Cyberbezpieczny Samorząd” odbywa się w formie elektronicznej przez **Lokalny System Informatyczny (LSI),** który dostępny jest pod adresem: https://lsi.cppc.gov.pl/beneficjent

Wnioskodawca wypełniać będzie za pośrednictwem LSI:

Dane rejestracyjne (Przekazanie niezbędnych danych kontaktowych).

Formularz aplikacyjny o grant (Opisanie koncepcji realizacji grantu, wskazanie planowanych wydatków w ramach grantu).

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie – harmonogram Konkursu Grantowego

NASK

19.07.2023 r.

Ogłoszenie naboru, uruchomienie LSI i możliwości składania wniosków.

13.10.2023 r.

do godziny 16.00

Zakończenie naboru i składania wniosków.

Okres kwalifikowalności wydatków - od dnia

01.06.2023 r.

i kończy się maksymalnie w ciągu 24 miesięcy od dnia wejścia w życie Umowy o powierzenie grantu (jednak nie później niż w dniu 30.06.2026 r.).

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie – podmioty uprawnione

NASK

Projekt będzie realizowany na terenie całego kraju. Zostaną nim objęte wszystkie jednostki samorządowe tj.

2 477	314	16
GMIN	POWIATÓW	WOJEWÓDZTW

2 807 JST

ŁĄCZNIE

Grupą docelową projektu jest administracja publiczna:

jednostki samorządu terytorialnego (JST) wraz z jednostkami podległymi

(z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia).

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie – alokacja

NASK

Alokacja na Granty w konkursie “Cyberbezpieczny Samorząd” wynosi

1 762 235 453,00 PLN

w tym środki unijne w wysokości

1 465 303 702,00 PLN

oraz

środki z budżetu państwa w wysokości

296 931 751,00 PLN

Maksymalna intensywność dofinansowania projektu grantowego może wynosić do

100%

kosztów kwalifikowalnych

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD

O projekcie – poziom dofinansowania

NASK

GMINY

od 200 000 PLN
do 850 000 PLN

Przedział wysokości dofinansowania grantu

POWIATY

do 850 000 PLN

Wysokość dofinansowania grantu

SAMORZĄDY WOJEWÓDZKIE

do 850 000 PLN

Wysokość dofinansowania grantu

Maksymalna kwota dofinansowania dla każdej JST jest wskazana w dokumentacji konkursowej

Załącznik nr 2 – Lista podmiotów uprawnionych do uczestniczenia w naborze

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD
Dokumentacja konkursu grantowego

NASK

Dokumentacja znajduje się na stronie Konkursu:

https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

- ❑ Regulamin Konkursu Grantowego
  - ❑ Załącznik nr 1 Wzór Wniosku o przyznanie Grantu (Formularz Aplikacyjny)
  - ❑ Załącznik nr 2 Lista podmiotów uprawnionych do uczestniczenia w naborze
  - ❑ Załącznik nr 3 Kryteria wyboru projektów grantowych
  - ❑ Załącznik nr 4 Wzór umowy o powierzenie Grantu
  - ❑ Załącznik nr 5 Lista dokumentów niezbędnych do podpisania Umowy o powierzenie Grantu
  - ❑ Załącznik nr 6 Ankieta dojrzałości cyberbezpieczeństwa w jednostce samorządu terytorialnego (i jednostkach podległych)
  - ❑ Załącznik nr 7 Oświadczenie dotyczące kwalifikowalności podatku VAT
  - ❑ Załącznik nr 8 Klauzula informacyjna FERC
  - ❑ Załącznik nr 9 Opis wskaźników projektu „Cyberbezpieczny Samorząd”

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

Załącznik nr 1 Wzór Wniosku o przyznanie Grantu (Formularz Aplikacyjny)

Koncepcja realizacji projektu	

Instrukcja LSI

- wypełnić znakami (system automatycznie liczy znaki)

Koncepcja realizacji *
Wpisz koncepcję realizacji

Rysunek 61 Widok formularza – pole do wypełnienia

Koncepcja realizacji projektu musi opisywać kontekst: z czego wynika potrzeba zmiany (np. ankiety, wnioski pokontrolne/doskonalące, plany/analizy własne/audyty), jaki jest obszar zmiany i jakiej zmiany dotyczy projekt.
Wskazówki wypełnienia i przykładowe opisy znajdują się w LSI – „Instrukcja dla Grantobiorców" w rozdziale 5.1.2.

Załącznik nr 1 Wzór Wniosku o przyznanie Grantu (Formularz Aplikacyjny)

ZAKRES RZECZOWY PROJEKTU	
Zadanie	**Nazwa zadania**
Zadanie 1	<tekst> 500 znaków

Instrukcja LSI

Instrukcja LSI w rozdziale 5.1.3 opisuje sposób zdefiniowania kosztów w ramach zadań.

Załącznik nr 2 Lista podmiotów uprawnionych do uczestniczenia w naborze

Gmina | Powiat | Województwo

Kwota dofinansowania (UE + BP)	Wkład UE	Wkład BP	Wkład własny JST
850 000,00 zł	722 500,00 zł	127 500,00 zł	84 066,00 zł
850 000,00 zł	705 500,00 zł	144 500,00 zł	- zł
850 000,00 zł	739 500,00 zł	110 500,00 zł	127 011,00 zł
850 000,00 zł	688 500,00 zł	161 500,00 zł	- zł
850 000,00 zł	705 500,00 zł	144 500,00 zł	54 255,00 zł
850 000,00 zł	697 000,00 zł	153 000,00 zł	- zł
850 000,00 zł	714 000,00 zł	136 000,00 zł	63 978,00 zł
850 000,00 zł	697 000,00 zł	153 000,00 zł	- zł

Kwota dofinansowania składa się z wkładu UE w ramach finansowania z FERC oraz wkładu z budżetu państwa. Dodatkowo niektóre JST zobligowane są do wniesienia wkładu własnego we wskazanej minimalnej kwocie. Kwota wynikająca z sumy kwoty dofinansowania i wkładu własnego jest maksymalną wysokością kosztów kwalifikowanych. W przypadku mniejszych projektów kwoty przelicza się proporcjonalnie.

Załącznik nr 3 Kryteria wyboru projektów grantowych

6	Zasadność kosztów w projekcie	Weryfikacji podlega czy Wnioskodawca wystarczająco uzasadnił potrzebę wskazanych wydatków oraz ich racjonalność w kontekście celu projektu oraz potrzeb Grantobiorcy.	0-1

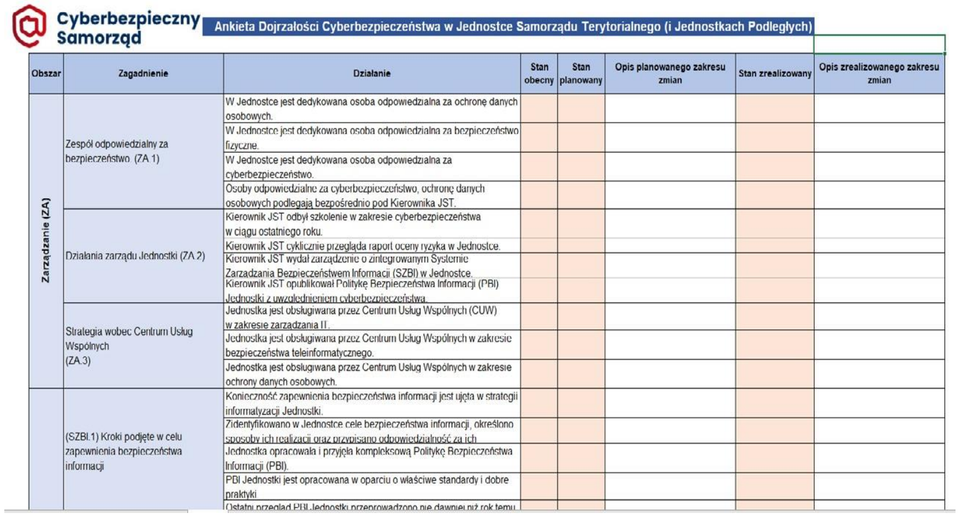
8	Opis koncepcji projektu	Weryfikacji podlega, czy Wnioskodawca przedstawił opis koncepcji projektu zawierający informacje o: - potrzebach Wnioskodawcy w zakresie cyfryzacji urzędu w tym zwiększenia poziomu bezpieczeństwa informacji urzędu, a także jednostek podległych (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia) - jeśli dotyczy; - celach i efektach projektu, w tym w odniesieniu do celów Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2;	0-1

Wszystkie kryteria punktowane są 0-1. Najważniejsze z punktu widzenia merytorycznej oceny są kryteria 6 i 8. Prosimy o szczególne zweryfikowanie swoich projektów pod kątem zgodności z tymi kryteriami.

CYBERBEZPIECZNY SAMORZĄD
Dokumentacja konkursu grantowego

NASK

Załącznik nr 6 Ankieta dojrzałości cyberbezpieczeństwa w jednostce samorządu terytorialnego (i jednostkach podległych)



Cyberbezpieczny Samorząd

Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)

Obszar	Zagadnienie	Działanie	Stan obecny	Stan planowany	Opis planowanego zakresu zmian	Stan zrealizowany	Opis zrealizowanego zakresu zmian
Zarządzanie (ZA)	Zespół odpowiedzialny za bezpieczeństwo. (ZA.1)	W Jednostce jest dedykowana osoba odpowiedzialna za ochronę danych osobowych.					
		W Jednostce jest dedykowana osoba odpowiedzialna za bezpieczeństwo fizyczne.					
		W Jednostce jest dedykowana osoba odpowiedzialna za cyberbezpieczeństwo.					
		Osoby odpowiedzialne za cyberbezpieczeństwo, ochronę danych osobowych podlegają bezpośrednio pod Kierownika JST.					
	Działania zarządu Jednostki (ZA.2)	Kierownik JST odbył szkolenie w zakresie cyberbezpieczeństwa w ciągu ostatniego roku.					
		Kierownik JST cyklicznie przegląda raport oceny ryzyka w Jednostce.					
		Kierownik JST wydał zarządzenie o zintegrowanym Systemie Zarządzania Bezpieczeństwem Informacji (SZBI) w Jednostce.					
		Kierownik JST opublikował Politykę Bezpieczeństwa Informacji (PBI) Jednostki z uwzględnieniem cyberbezpieczeństwa.					
	Strategia wobec Centrum Usług Wspólnych (ZA.3)	Jednostka jest obsługiwana przez Centrum Usług Wspólnych (CUW) w zakresie zarządzania IT.					
		Jednostka jest obsługiwana przez Centrum Usług Wspólnych w zakresie bezpieczeństwa teleinformatycznego.					
		Jednostka jest obsługiwana przez Centrum Usług Wspólnych w zakresie ochrony danych osobowych.					
	(SZBI.1) Kroki podjęte w celu zapewnienia bezpieczeństwa informacji	Konieczność zapewnienia bezpieczeństwa informacji jest ujęta w strategii informatyzacji Jednostki.					
		Zidentyfikowano w Jednostce cele bezpieczeństwa informacji, określono sposoby ich realizacji oraz przypisano odpowiedzialność za ich					
		Jednostka opracowała i przyjęła kompleksową Politykę Bezpieczeństwa Informacji (PBI).					
		PBI Jednostki jest opracowana w oparciu o właściwe standardy i dobre praktyki					
		Ostatni przegląd PBI Jednostki przeprowadzono nie dawniej niż rok temu					

- Narzędzie ułatwiające **określenie aktualnej pozycji na ścieżce rozwoju JST** oraz **stanu docelowego** jaki jednostka zamierza osiągnąć przy wsparciu z projektu.
- To także mechanizm pozwalający **udokumentować rzeczywistą poprawę obszarze cyberbezpieczeństwa** wymagany do rozliczenia projektów.
- **Wymagane jest jej wypełnienie i dostarczenie 2 razy:** do 30 dni od podpisania umowy wraz z raportem końcowym po zakończeniu projektu grantowego

Ankieta jest bardzo szeroka i nie oznacza, że zamierzeniem projektu jest realizacja wszystkich wymienionych jej działań. Wybór działań, które będą zrealizowane lub doskonalone jest elementem planowania, który wynika z wewnętrznych opracowań np. audytów, wniosków pokontrolnych i analiz ryzyka.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

CYBERBEZPIECZNY SAMORZĄD
Dokumentacja konkursu grantowego

NASK

Załącznik nr 9 Opis wskaźników projektu Cyberbezpieczny Samorząd

Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym…

Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym…

Wskaźnik obejmuje pracowników informatycznych podmiotów wykonujących zadania publiczne (Grantobiorcy), (nie będących pracownikami IT), objętych wsparciem szkoleniowym, podnoszącym umiejętności z zakresu ICT.

Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji

Przez system teleinformatyczny należy rozumieć zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne.

Wskaźnik obejmuje wdrożenie lub rozbudowę lub unowocześnienie systemu teleinformatycznego.

Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych

Roczna liczba użytkowników nowo opracowanych lub znacząco zmodernizowanych publicznych usług, produktów i procesów cyfrowych.

Znaczące modernizacje obejmują tylko nowe funkcjonalności.

W ramach wskaźnika wykazuje się użytkowników e-usług, a także liczbę pobrań/uruchomień/odtworzeń.

Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST

Wskaźnik obejmuje liczbę podmiotów wspartych w JST. Do wartości wskaźnika należy wliczyć jednostki podległe JST (z ograniczeniem do jednostek sektora publicznego i z wyłączeniem POZ).

Wskaźnik mierzalny na etapie rozliczenia końcowego. We wniosku rozliczeniowym każde JST zobowiązane będzie do podsumowania działań, jakie podjął i sfinansował w ramach projektu grantowego, w tym wskaże jakie jednostki podległe zostały objęte wsparciem.

Wskazanie aktualnego stanu realizacji wskaźników projektu będzie konieczne w czasie trwania (monitorowanie) i na zakończenie (rozliczenie) projektu.

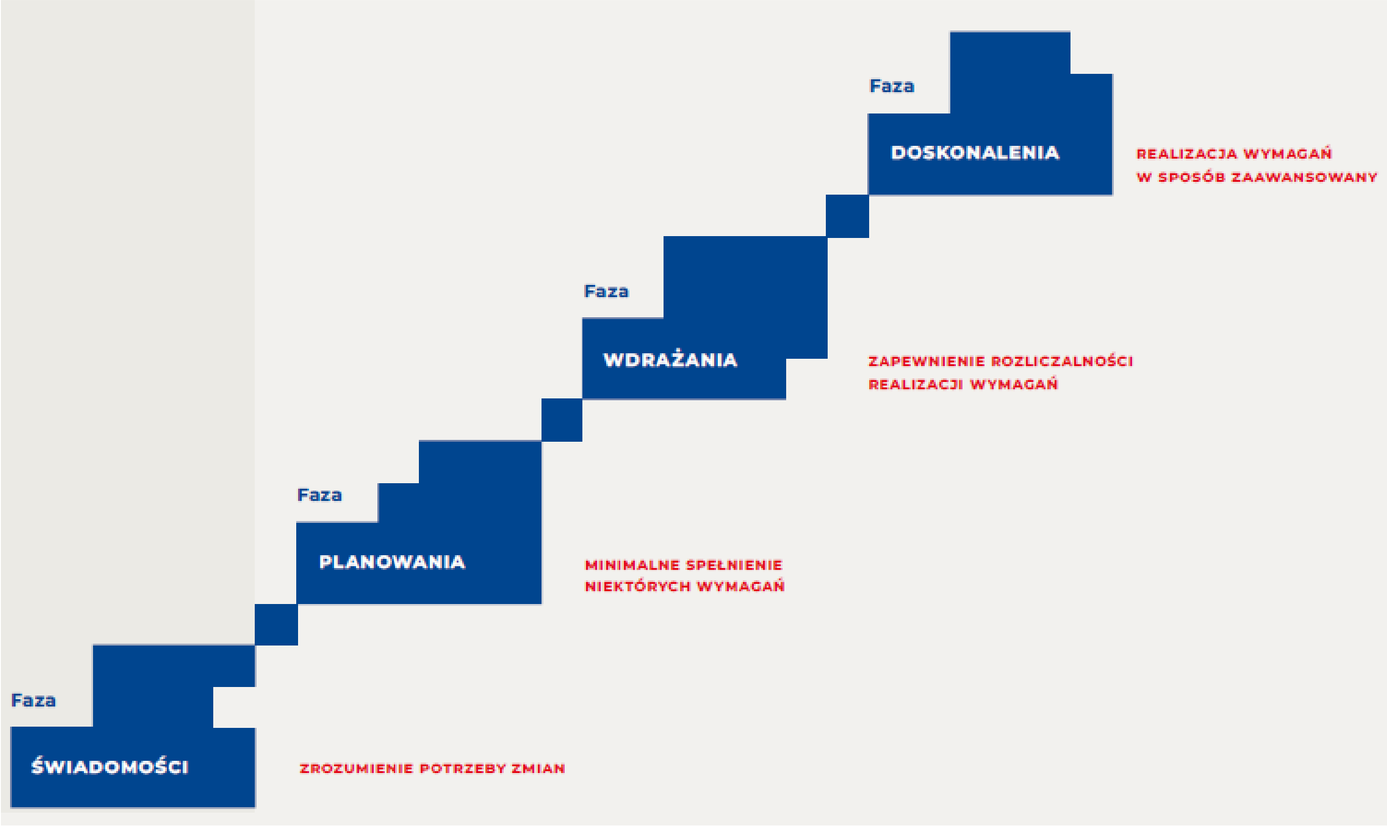
Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA

Kilka słów o dojrzałości

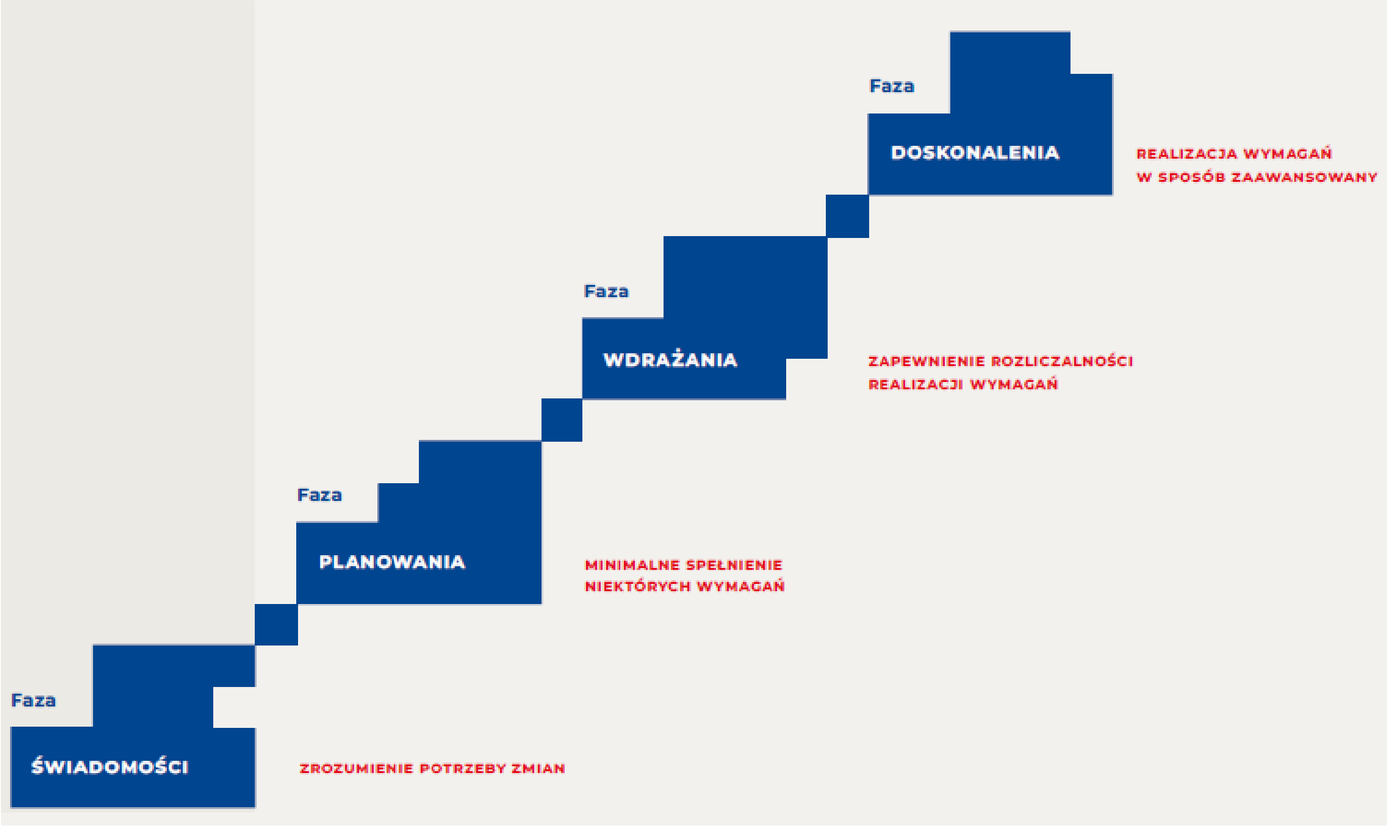


Brak polityki i procedur bezpieczeństwa w JST stanowi istotne zagrożenie dla jej funkcjonowania. Gdy kierownictwo nie uznaje inwestycji w systemy związane z bezpieczeństwem informacji za nieodzowne w kontekście wykonywania zadań publicznych, zwiększa się ryzyko naruszenia bezpieczeństwa danych. Ponadto brak oceny wpływu własnych podatności na realizację zadań oraz niewłaściwe zrozumienie ryzyka związanego z lukami w zabezpieczeniach może prowadzić do poważnych konsekwencji dla jednostki.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA

Kilka słów o dojrzałości



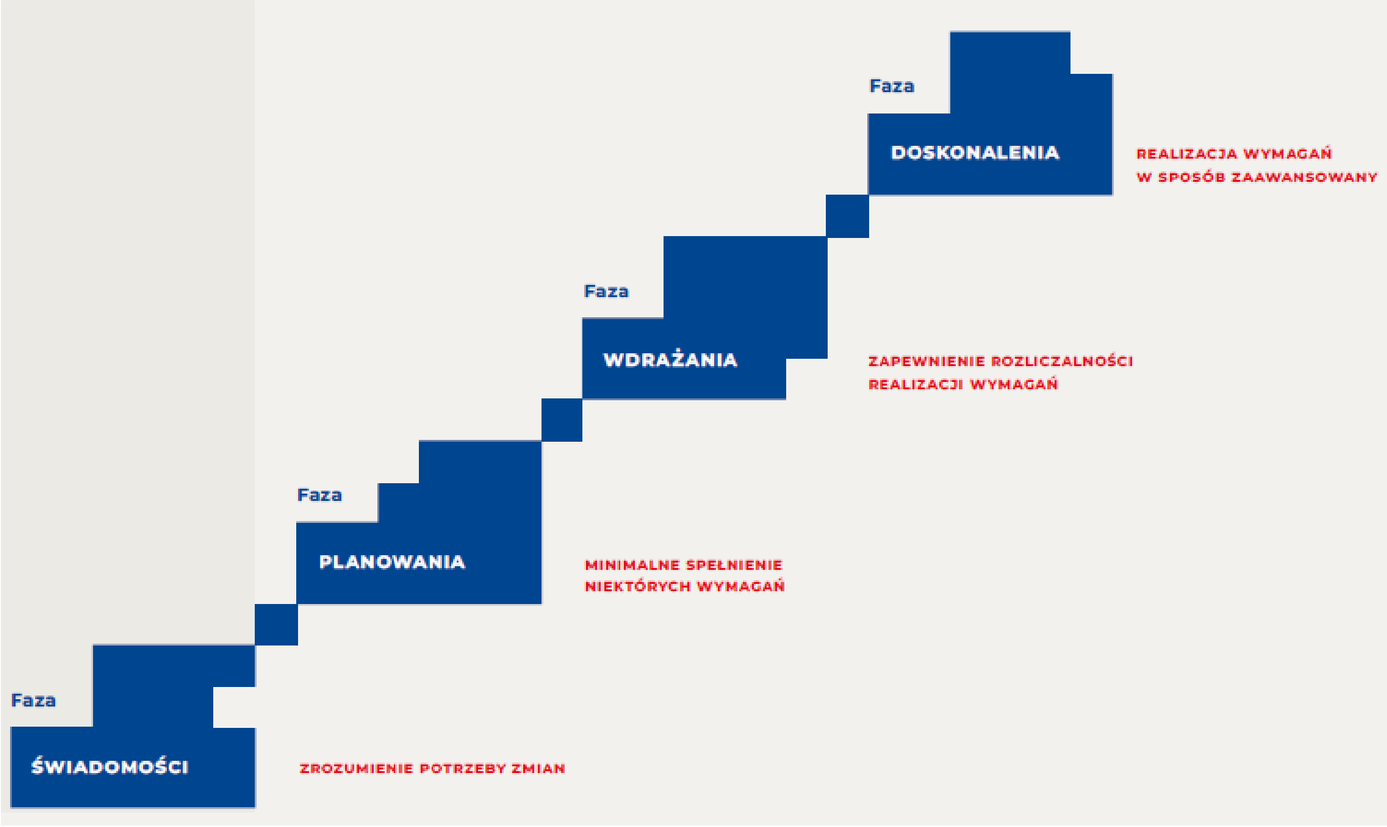
Faza I. ZROZUMIENIE POTRZEBY ZMIAN

To początkowy etap ścieżki rozwoju cyberbezpieczeństwa. W tej fazie znajdują się jednostki, które dopiero nabierają świadomości istnienia zagrożeń cyberbezpieczeństwa i **działają intuicyjnie, niespójnie, ad hoc oraz wyłącznie reaktywnie** odpowiadają na wykryte incydenty lub w ogóle nie są ich świadome. Zaczynają rozpoznawać ryzyko dla realizacji zadań publicznych wynikające ze słabości zabezpieczeń. Nie mają zdefiniowanych zasad, procedur, polityk ani SZBI chroniących informacje oraz dysponują tylko niezbędnymi dla funkcjonowania wdrożeniami technicznymi, które nie uwzględniają wielu zagadnień cyberbezpieczeństwa.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA

Kilka słów o dojrzałości



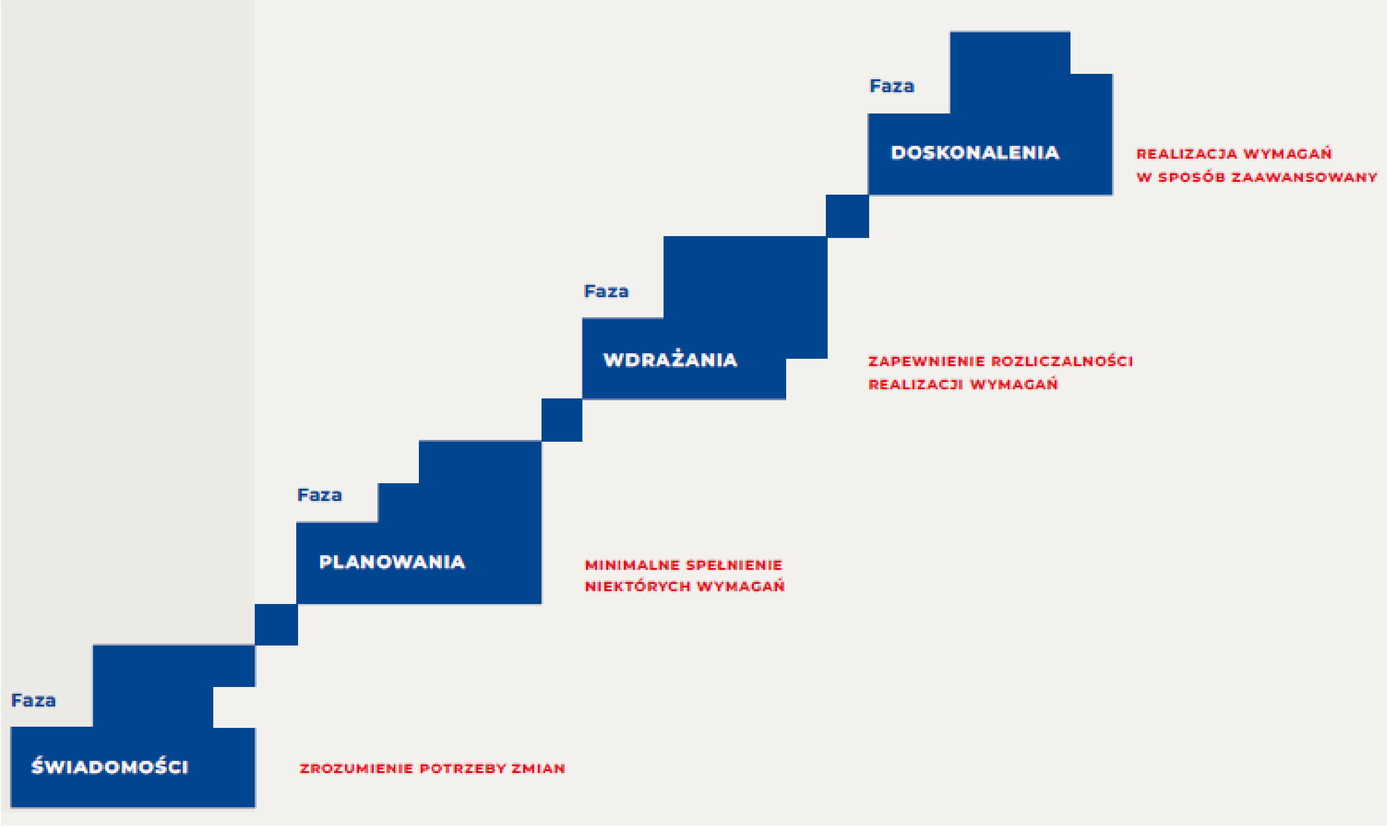
Faza II. MINIMALNE SPEŁNIENIE NIEKTÓRYCH WYMAGAŃ

Ta faza charakteryzuje jednostkę, która chroni swoją infrastrukturę i **zapewnia jej częściową ciągłość** realizowania zadań publicznych (przynajmniej w minimalnym stopniu). JST w tej fazie jest **świadoma zagrożeń** i konieczności zapobiegania im oraz w pewnym stopniu podejmuje takie działania, wykorzystując kompetencje specjalistów, własne procedury i posiadane narzędzia. **Wdrożone są mechanizmy bezpieczeństwa używanych aplikacji i sieci**, ale zmiany w tym zakresie nie są zarządzane centralnie – powszechne są działania ad hoc. W tym stanie przeważa model, w którym **instytucja ufa interakcji między użytkownikiem a systemami**. Programy budowania świadomości na temat cyberzagrożeń są rozważne tylko w przypadku kluczowych pracowników, procedury bezpieczeństwa informacji są zdefiniowane nieformalnie, a analizę ryzyka przeprowadza się jedynie w ograniczonym zakresie.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA

Kilka słów o dojrzałości



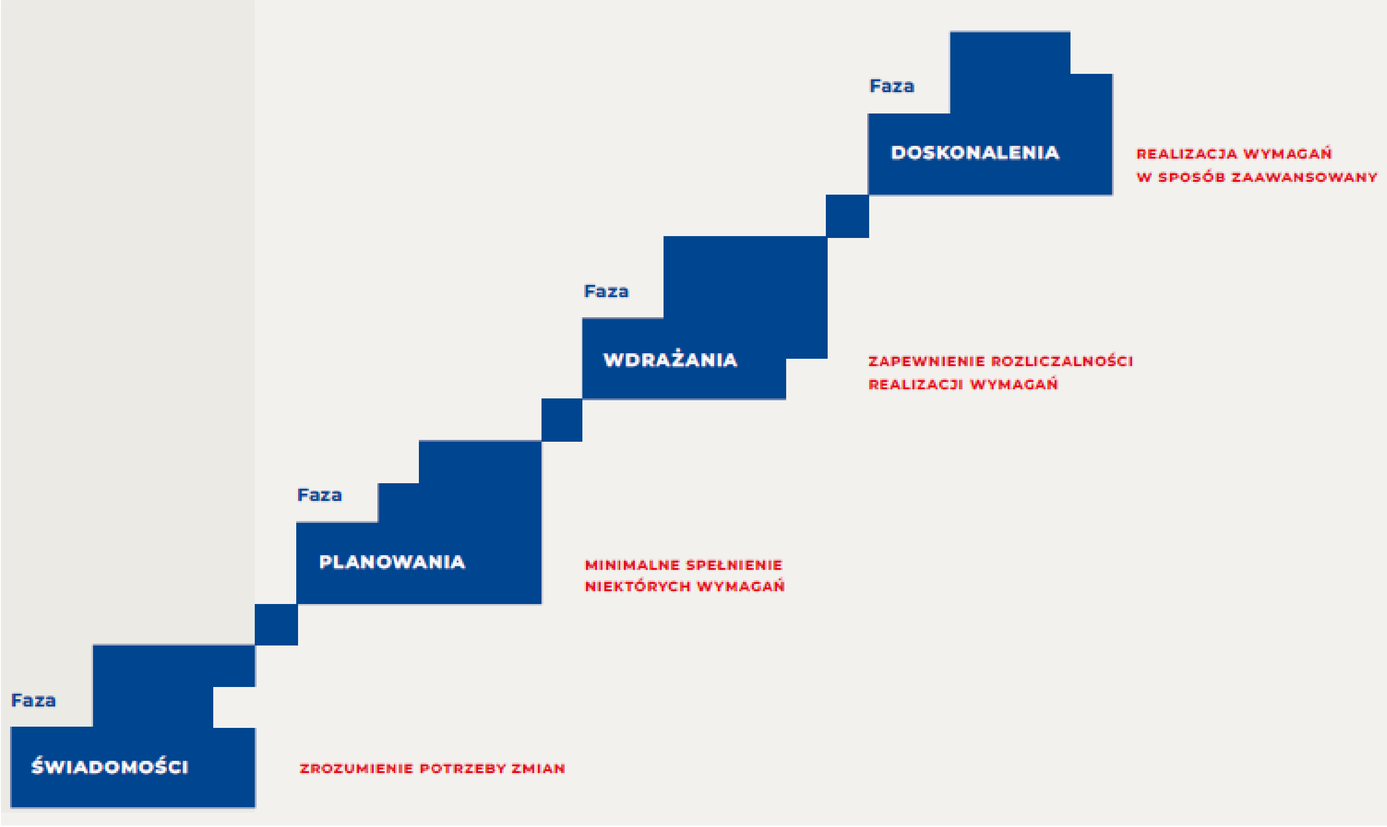
Faza III. ZAPEWNIENIE ROZLICZALNOŚCI REALIZACJI WYMAGAŃ

W tej fazie JST posiadają wybrane polityki związane z bezpieczeństwem informacji. Niektóre aspekty interakcji użytkowników z systemami informacyjnymi są postrzegane jako potencjalne ryzyka. Tutaj **nie podejmuje się już działań ad hoc** – praca oparta jest na planowaniu lub wykorzystywaniu istniejących polityk, procedur, udokumentowanych procesów. Modele konfiguracji są wdrażane centralnie, stosowane są zasady bezpieczeństwa i procedury postępowania, stale rozwijana jest świadomość użytkowników, a zgodność JST z regulacjami wzrasta. Kontrole dostępu do informacji są obowiązkowe i ściśle monitorowane. Środki bezpieczeństwa wprowadza się na zasadzie oceny kosztu i korzyści chronionych informacji.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA

Kilka słów o dojrzałości



Faza IV. REALIZACJA WYMAGAŃ W SPOSÓB ZAAWANSOWANY

Ta faza charakteryzuje się najogólniej **zgodnością z wymaganiami KRI oraz uoKSC**. Oznacza m.in. posiadanie kontroli nad bezpieczeństwem informacji w obrębie jednostki, monitorowaniem systemów, utrzymywaniem wysokiej świadomości zagrożeń i zdolności do reagowania na nie lub zapobiegania im. W JST w tej fazie istnieje kompleksowy plan utworzony na podstawie formalnych zasad i procedur operacyjnych, mających na celu zapobieganie, wykrywanie i korygowanie wykrytych problemów bezpieczeństwa. Aby jednostka miała pełną zgodność, zarządzanie bezpieczeństwem **musi polegać na identyfikowaniu wszelkich symptomów związanych z naruszeniem bezpieczeństwa, a wykryte incydenty muszą być obsługiwane w zorganizowany sposób**. Zaawansowany poziom dotyczy również architektury bezpieczeństwa informacji w jednostce. **Istnieje system zapewniający identyfikowalność zbiorów informacji, użytkowników, systemów, urządzeń i oprogramowania**.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA

Kilka słów o normach i metodykach

NASK

Planując rozwój w obszarze bezpieczeństwa informacji w JST można polegać na normach:

PN-ISO/IEC 27001 określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w organizacji,

NCS-200 „Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych”.

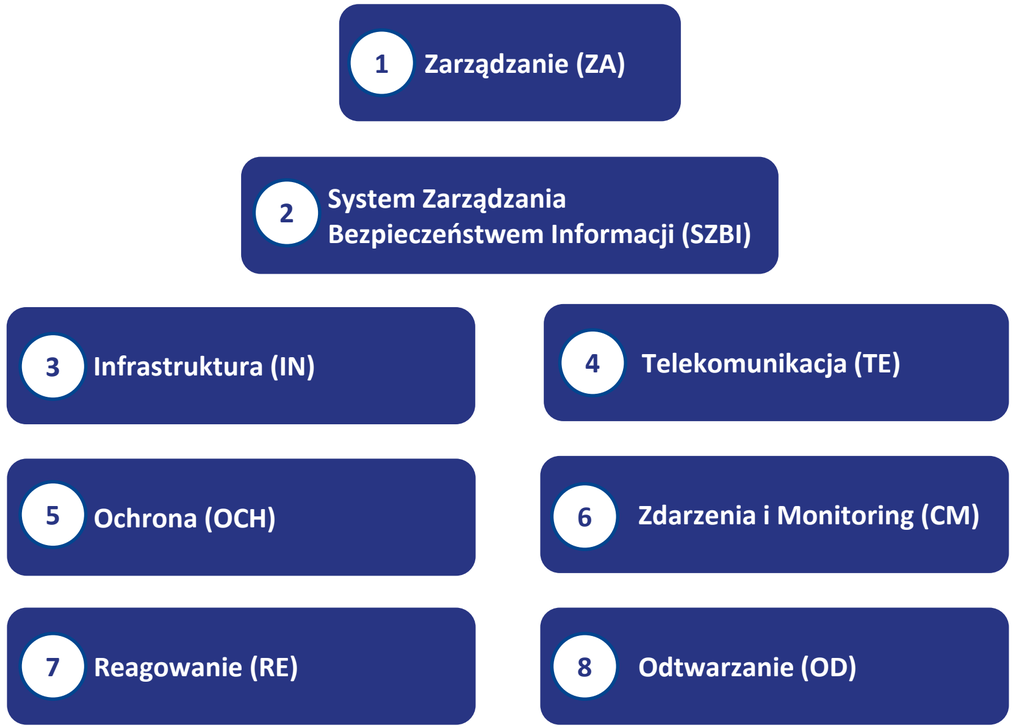
Można inspirować się także modelami dojrzałości:

C2M2 (Cybersecurity Capability Maturity Model) narzędzie, które pomaga organizacjom ocenić ich możliwości w zakresie cyberbezpieczeństwa i zoptymalizować inwestycje w zabezpieczenia,

SIM3 (Security Incident Management Maturity Model) to narzędzie do zorganizowania zarządzania incydentami.

People Capability Maturity Model, IoT Security Maturity Model, Cloud Security Maturity Model, Data Security Maturity Model…

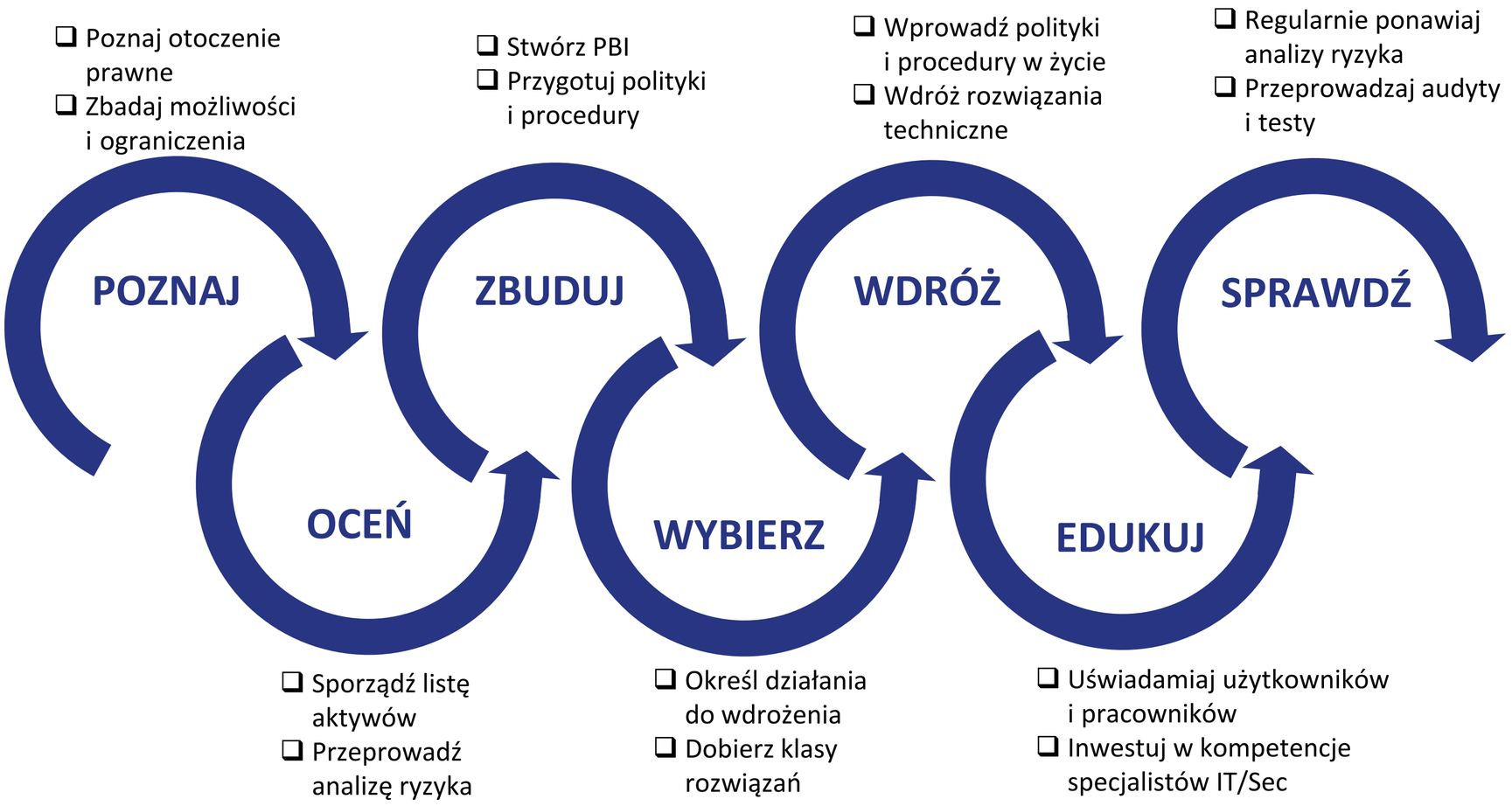
Na potrzeby projektu zaproponowano, w Ankiecie Dojrzałości Cyberbezpieczeństwa w JST, uproszczony model składający się z propozycji 136 działań w ramach 8 podstawowych zagadnień.



Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA

Przyda się Roadmapa



Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA | NASK

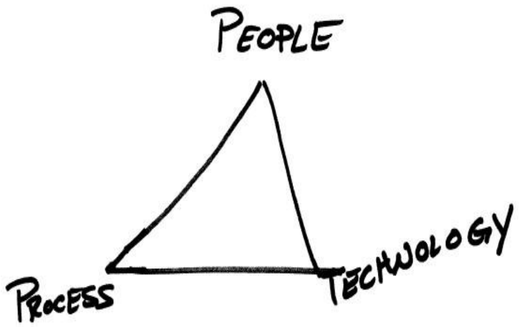
Uzasadnienie i monitorowanie projektu

IDENTYFIKACJA POTRZEB

Plan budowy/aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji

Wyniki kontroli NIK z 2019r.
„Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”

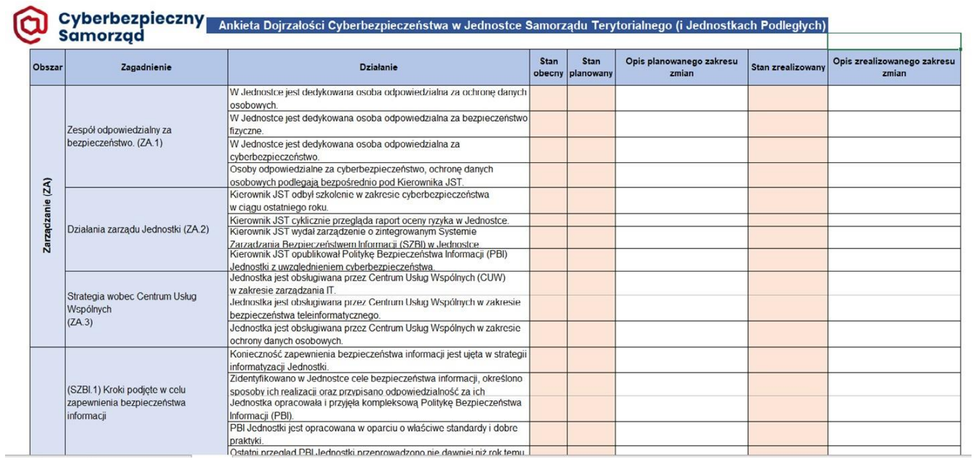
Zlecone dodatkowe testy, badania i audyty



OKREŚLENIE AKTUALNEJ I DOCELOWEJ POZYCJI

Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)

(Załącznik nr 6 do Regulaminu Konkursu Grantowego)



Cyberbezpieczny Samorząd

Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)

Obszar	Zagadnienie	Działanie	Stan obecny	Stan planowany	Opis planowanego zakresu zmian	Stan zrealizowany	Opis zrealizowanego zakresu zmian
Zarządzanie (ZA)	Zespół odpowiedzialny za bezpieczeństwo. (ZA.1)	W Jednostce jest dedykowana osoba odpowiedzialna za ochronę danych osobowych.					
		W Jednostce jest dedykowana osoba odpowiedzialna za bezpieczeństwo fizyczne.					
		W Jednostce jest dedykowana osoba odpowiedzialna za cyberbezpieczeństwo.					
		Osoby odpowiedzialne za cyberbezpieczeństwo, ochronę danych osobowych podlegają bezpośrednio pod Kierownika JST.					
	Działania zarządu Jednostki (ZA.2)	Kierownik JST odbył szkolenie w zakresie cyberbezpieczeństwa w ciągu ostatniego roku.					
		Kierownik JST cyklicznie przegląda raport oceny ryzyka w Jednostce.					
		Kierownik JST wydał zarządzenie o zintegrowanym Systemie Zarządzania Bezpieczeństwem Informacji (SZBI) w Jednostce.					
		Kierownik JST opublikował Politykę Bezpieczeństwa Informacji (PBI) Jednostki z uwzględnieniem cyberbezpieczeństwa.					
	Strategia wobec Centrum Usług Wspólnych (ZA.3)	Jednostka jest obsługiwana przez Centrum Usług Wspólnych (CUW) w zakresie zarządzania IT.					
		Jednostka jest obsługiwana przez Centrum Usług Wspólnych w zakresie bezpieczeństwa teleinformatycznego.					
		Jednostka jest obsługiwana przez Centrum Usług Wspólnych w zakresie ochrony danych osobowych.					
	(SZBI.1) Kroki podjęte w celu zapewnienia bezpieczeństwa informacji	Konieczność zapewnienia bezpieczeństwa informacji jest ujęta w strategii informatyzacji Jednostki.					
		Zidentyfikowano w Jednostce cele bezpieczeństwa informacji, określono sposoby ich realizacji oraz przypisano odpowiedzialność za ich					
		Jednostka opracowała i przyjęła kompleksową Politykę Bezpieczeństwa Informacji (PBI).					
		PBI Jednostki jest opracowana w oparciu o właściwe standardy i dobre praktyki.					
		Ostatni przegląd PBI Jednostki przeprowadzono nie dawniej niż rok temu					

UWZGLĘDNIENIE DOBRYCH PRAKTYK

Rozdział 8 Poradnika przybliża kilka dobrych praktyk, które warto rozważyć na etapie planowania rozwoju.

Mogą one być inspirujące do podjęcia decyzji efektywnych operacyjnie i ekonomicznie, zarówno na etapie realizacji projektu grantowego jak i później w fazie utrzymania jego efektów i dłuższym horyzoncie czasowym.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PLANOWANIE ROZWOJU JST W OBSZARZE CYBERBEZPIECZEŃSTWA

Ryzyka dla projektu

- ❑ Zakup nieadekwatnych, nieuzasadnionych rozwiązań
- ❑ Wdrożenie rozwiązań bez pespektyw budżetu na ich utrzymanie po zakończeniu projektu
- ❑ Wydanie grantu na bieżące potrzeby bez inwestycji w zmianę stanu rzeczy
- ❑ Wydanie środków na potrzeby nie wspierające bezpośrednio poprawy bezpieczeństwa teleinformatycznego
- ❑ Zbudowanie SZBI „na papierze” bez szans na jego realne działanie i doskonalenie

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PORADNIK

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PORADNIK

Poradnik do pobrania na stronie projektu:

https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

PORADNIK

Rozdział 6. Wykaz wymagań bezpieczeństwa dla podmiotów publicznych

NASK

Na szczególną uwagę zasługuje **Rozdział 6.** Wykaz wymagań bezpieczeństwa dla podmiotów publicznych, który:

Zawiera wykaz wymagań prawnych w zakresie bezpieczeństwa teleinformatycznego wobec podmiotów JST (KRI i uoKSC)

Wyjaśnia, doprecyzowuje te wymagania Wskazuje przykłady, rekomendowane działania, których podjęcie wpłynie na zrealizowanie wymagania lub podniesie dojrzałość dotychczasowej realizacji.

Mając na uwadze dużą liczbę podmiotów uprawnionych, różną specyfikę organizacyjną, przeróżną architekturę teleinformatyczną, itd. itp. **nie jest możliwe zaproponowanie jednolitego podejścia do budowania cyberbezpieczeństwa w podmiocie administracji samorządowej i/lub jednostkach podległych.**

W zamian zaproponowany został obszerny zbiór wiedzy, z której można czerpać budując własną strategię.

Poradnik stanowi materiał dodatkowy, w konkursie pierwszeństwo ma Regulamin Konkursu Grantowego wraz z załącznikami.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Główne wyzwania

NASK

TECHNICZNE

- identyfikacja co i dlaczego chronimy?
- dobór klas rozwiązań
- zapewnienie ciągłości monitorowania
- utrzymanie zdolności do szybkiej reakcji

ORGANIZACYJNE

- wsparcie kierownictwa
- przygotowanie jednostki
- dyscyplina i higiena
- sprawność operacyjna

KOMPETENCYJNE

- budowanie świadomości
- kompetencje specjalistyczne
- weryfikowanie odporności

Jak zbudować System?

który chroni to co trzeba tak jak trzeba → który jest trwały i nie tylko na papierze → który dba o każde ogniwo

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Wydatki w obszarze organizacyjnym

NASK

OBSZAR ORGANIZACYJNY:

Opracowanie, wdrożenie oraz aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Wprowadzenie lub aktualizacja:

- polityk bezpieczeństwa informacji (PBI),
- analizy ryzyka (w tym opracowanie i wdrożenie metodyk).

Deklaracja stosowania, np.

- procedury eksploatacyjne,
- procedury ciągłości działania biznesowego po katastrofie,
- procedury zasad monitorowania infrastruktury,
- procedury obsługi incydentów.

Audyt Systemu Zarządzania Bezpieczeństwem Informacji

Audyt zgodności z KRI/UoKSC przez wykwalifikowanych audytorów

(Re)certyfikacja SZBI na zgodność z normami 27001, 22301.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Wydatki w obszarze kompetencyjnym

NASK

OBSZAR KOMPETENCYJNY:

Podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST.

Szkolenia z zakresu cyberbezpieczeństwa dla pracowników JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji.

Szkolenia specjalistyczne dla kadry zarządzającej i obsługi informatycznej w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach projektu grantowego.

Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Wydatki w obszarze technicznym

NASK

OBSZAR TECHNICZNY:

Zakup, wdrożenie i utrzymanie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa, z niezbędnym wsparciem producenta.

Zakup, wdrożenie i utrzymanie rozwiązań ciągłego monitorowania bezpieczeństwa, skanery podatności, zarządzanie podatnościami, zarządzanie zasobami IT i aktywami podlegającymi ochronie.

Zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa.

Zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby centrów cyberbezpieczeństwa (SOC), także jako element Centrum Usług Wspólnych, zakup testów i badań bezpieczeństwa, dostępu do informacji bezpieczeństwa oraz inne usługi integracyjne dotyczące obszaru cyberbezpieczeństwa.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Katalog sprzętu, urządzeń bezpieczeństwa i oprogramowania

NASK

Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X

Firewall sieciowy WAF (Web Application Firewall)

SIEM (Security Information and Event Management)

UTM (Unified Threat Management)

IPS (Intrusion Prevention System)

IDS (Intrusion Detection System)

VPN (Virtual Private Network)

NAC (Network Access Control)

Proxy sprzętowe

Serwer

Serwer do wykonywania kopii zapasowych

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Katalog sprzętu, urządzeń bezpieczeństwa i oprogramowania

NASK

Dyski twarde do macierzy dyskowej

Macierz dyskowa

Network Attached Storage (NAS)

Storage Area Network (SAN)

Web Secure Gateway

Email Secure Gateway

Generator prądu. UPS

Ochrona AntyDDoS

Oprogramowanie antywirusowe

Oprogramowanie typu EDR (Endpoint Detection and Response)

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Katalog sprzętu, urządzeń bezpieczeństwa i oprogramowania

NASK

Oprogramowanie typu XDR (Extended Detection and Response)

Oprogramowanie do wykonywania kopii zapasowych.
Oprogramowanie antyspamowe
Oprogramowanie Menadżera logów.

Oprogramowanie do zarządzania podatnościami.

Oprogramowanie przeciwdziałającemu wyciekowi danych (DLP - Data Leak Prevention)

Oprogramowanie do zarządzania uprzywilejowanemu dostępowi (PAM- Privileged Access Management)

Oprogramowanie do zarządzania tożsamością i dostępem

Oprogramowanie centralnego menadżera haseł

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

Katalog sprzętu, urządzeń bezpieczeństwa i oprogramowania

NASK

Oprogramowanie do monitorowania infrastruktury informatycznej

Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych

Oprogramowanie do badania podatności systemów informatycznych w tym WWW

Oprogramowanie do badania podatności w kodzie aplikacji

Oprogramowanie typu sandbox do badania bezpieczeństwa aplikacji oraz plików

Oprogramowanie do analizy powłamaniowej

Oprogramowanie do ochrony przed ransomware

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

KATALOG KOSZTÓW KWALIFIKOWANYCH

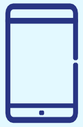
Przykładowe usługi zewnętrzne

NASK

Usługa poczty elektronicznej w chmurze obliczeniowej typu IaaS, SaaS, PaaS z elementami bezpieczeństwa.

Usługa testowania bezpieczeństwa infrastruktury sieciowej.

Usługa testowania bezpieczeństwa serwisów internetowych.



Usługa testowania bezpieczeństwa aplikacji.

Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS w zakresie sandbox do badania bezpieczeństwa aplikacji oraz plików.

Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

~~KATALOG KOSZTÓW KWALIFIKOWANYCH~~

Uwaga na wydatki NIEKWALIFIKOWANE!

NASK

Stacje robocze lub laptopy.

Urządzenia mobilne tj. smartfony lub tablety.

Akcesoria i urządzenia peryferyjne np.

drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki, klawiatury, myszy.

Materiały eksploatacyjne.

Oprogramowanie biurowe, z wyłączeniem:

systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa.

Szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np.

szkolenia z obsługi oprogramowania biurowego.

Usługi dostępu do internetu, abonamenty telefoniczne.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

LOKALNY SYSTEM INFORMATYCZNY (LSI)

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

LOKALNY SYSTEM INFORMATYCZNY (LSI)

Zakładanie konta

NASK

Instrukcja LSI Grantobiorcy jest dostępna na stronie internetowej naboru.
https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

Wniosek o przyznanie Grantu należy wypełnić za pomocą LSI - https://lsi.cppc.gov.pl/beneficjent

Aby zarejestrować użytkownika w LSI wejdź na stronę https://lsi.cppc.gov.pl.

Wybierz opcję Utwórz konto.

Konto może utworzyć każda osoba upoważniona przez JST.

Pamiętaj! Do zarejestrowania użytkownika potrzebna jest autoryzacja przez Krajowy Węzeł Identyfikacji Elektronicznej.

Wniosek podpisywany jest przez aplikację **Podpis GOV**.

Ważne! Wniosek powinien podpisać wyznaczony pracownik JST lub osoba upoważniona do reprezentowania Grantobiorcy.

Dopiero na etapie podpisywania Umowy będzie wymagany podpis włodarza i skarbnika.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

LOKALNY SYSTEM INFORMATYCZNY (LSI)

Obsługa wniosku

NASK

Po zalogowaniu się do LSI jest możliwość składania wniosków o przyznanie grantu, edycji, sprostowania, usunięcia, wycofania wniosków oraz generowania z nich plików w formacie PDF.

Ważne!

Podczas podpisywania i wysyłania wniosku będzie potrzebna aplikacja **Podpis GOV**.

Aby utworzyć wniosek należy wejść na listę naborów, odszukać nabór nr FERC.02.02-CS.01-001/23 i kliknąć złóż wniosek.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

LOKALNY SYSTEM INFORMATYCZNY (LSI)

Składanie wniosku

NASK

Po zalogowaniu do LSI, wybierz
z Menu bocznego zakładkę **Lista naborów**
i wyszukaj odpowiedni nabór.

Pomogą Ci w tym pola Szukaj lub Wybierz, które umożliwiają filtrowanie po wartościach danej kolumny.

System wyświetli szczegóły naboru.
Z tego miejsca możesz wrócić do Listy naborów za pomocą przycisku Wróć do listy.
Przycisk Złóż wniosek umożliwia złożenie wniosku w danym naborze.

Lub

Po zalogowaniu do LSI, wybierz
z Menu bocznego zakładkę **Lista naborów**
i wyszukaj odpowiedni nabór.

W kolumnie Operacje kliknij Trzy pionowe kropki,
następnie przycisk **Złóż wniosek.**

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

LOKALNY SYSTEM INFORMATYCZNY (LSI)

Edycja wniosku

NASK

W systemie LSI jest możliwość edycji wniosku roboczego i złożonego (jeśli w procesie oceny ekspert odeśle wniosek do poprawy).

Aby edytować zapisany wniosek roboczy, z menu bocznego po lewej stronie, wybierz zakładkę **Twoje wnioski,** a następnie **Robocze.** System wyświetli Listę wniosków roboczych.

Przy odpowiednim wniosku kliknij przycisk **Edytuj.**

System wyświetli wniosek do uzupełnienia.

Pamiętaj!

Podczas wypełniania formularza pomocne są poniższe funkcjonalności:

Pobierz pdf wniosku

Sprawdź poprawność sekcji, grupy, formularza

Wyślij wniosek

Wyjdź z formularza

Zapisz wniosek/zmiany.

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

LOKALNY SYSTEM INFORMATYCZNY (LSI)

Edycja wniosku

NASK

Po wypełnieniu wszystkich pól, kliknij przycisk Zapisz zmiany.

Pamiętaj!

Opcja Zapisz zmiany powoduje zapisanie formularza w wersji roboczej.

Po kliknięciu przycisku Sprawdź poprawność formularza, jeśli wniosek wymaga dalszego uzupełnienia, pojawi się komunikat. Pola, które wymagają poprawy zaznaczone są czerwonym kolorem.

Jeśli wniosek jest poprawnie uzupełniony, kliknij przycisk Wyślij wniosek. System wyświetli komunikat sukcesu.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

LOKALNY SYSTEM INFORMATYCZNY (LSI)

Podpisywanie wniosku

- Po naciśnięciu przycisku **Wyślij wniosek** system automatycznie sprawdzi poprawność całego formularza wniosku, jeśli wniosek będzie zawierał błędy system wyświetli błędy i nie przejdzie do kolejnego kroku.
- Jeśli weryfikacja całego wniosku przebiegnie poprawnie, **system przejdzie do kolejnego kroku** – podpisywania. Uruchom aplikację Podpis GOV.

  Przed wysłaniem i podpisaniem możesz zapisać zmiany i pobrać pdf wniosku, aby mieć podgląd podpisywanego dokumentu (w aplikacji podpis.gov podgląd jest niedostępny).
- W aplikacji **Podpis GOV** kliknij przycisk **Wybierz certyfikat.**
- Następnie Aplikacja Podpis GOV wyświetli okno, gdzie wprowadzasz **PIN do podpisu.**
- W polu Podaj PIN wpisz **PIN do podpisu kwalifikowanego.** Kliknij przycisk Akceptuję.
- Wniosek został pomyślnie podpisany i wysłany. **Wniosek zmieni status na Wysłany.**

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

LOKALNY SYSTEM INFORMATYCZNY (LSI)

Podpisywanie wniosku – Aplikacja *Podpis GOV*

NASK

- Instrukcja użycia aplikacji Podpis GOV znajduje się:

https://epuap.gov.pl -> STREFA URZĘDNIKA -> POMOC -> Instrukcje i podręczniki

- Aplikację Podpis GOV pobieramy z:

https://pz.gov.pl -> Certyfikat kwalifikowany

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA

DZIĘKUJEMY ZA UWAGĘ

Centrum Projektów Polska Cyfrowa ul.
Spokojna 13A
01-044 Warszawa

NASK

Operator NASK - PIB - helpdesk Tel.:
+48 22 182 22 94

Infolinia działa w godzinach 8:00-16:00 od poniedziałku do piątku. e-mail:
cyberbezpiecznysamorzad@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy

Dofinansowane przez Unię Europejską

CENTRUM PROJEKTÓW POLSKA CYFROWA