

ZARZĄDZENIE NR 47/2026
STAROSTY TOMASZOWSKIEGO

z dnia 8 września 2026 r.

w sprawie wprowadzenia procedury monitorowania utrzymania efektów projektu „Cyberbezpieczny Samorząd”

Na podstawie art. 34 ust. 1, art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (t.j. Dz. U. z 2025r. poz. 1684 z późn. zm.) oraz § 13 ust. 1 umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1383/ FERC.02.02-CS.01-001/23/2024 w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 - Wzmocnienie krajowego systemu cyberbezpieczeństwa, zarządzam co następuje:

§ 1. Wprowadza się procedurę monitorowania utrzymania efektów projektu „Cyberbezpieczny Samorząd”, tj. utrzymania środków trwałych i usług nabytych w ramach projektu nr FERC.02.02-CS.01-001/23, pn.: "Cyberbezpieczny Samorząd" współfinansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 - Wzmocnienie krajowego systemu cyberbezpieczeństwa, która stanowi Załącznik nr 1 do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Sekretarzowi Powiatu Tomaszowskiego.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Starosta Tomaszowski

Dariusz Kowalczyk

Załącznik nr 1
do Zarządzenia Nr 47/2026
Starosty Tomaszowskiego
z dnia 8 września 2026 roku

PROCEDURA MONITOROWANIA UTRZYMANIA EFEKTÓW PROJEKTU „CYBERBEZPIECZNY SAMORZĄD”

1. Cel procedury

Celem procedury jest określenie zasad monitorowania, dokumentowania oraz potwierdzania utrzymania efektów projektu „Cyberbezpieczny Samorząd” przez cały okres jego trwałości, zgodnie z umową o powierzenie grantu, wytycznymi programu FERC oraz obowiązującymi przepisami prawa.

2. Zakres procedury

Procedura obejmuje działania związane z bieżącym monitorowaniem, nadzorem oraz utrzymaniem efektów projektu „Cyberbezpieczny Samorząd” w okresie jego trwałości, w szczególności:

- 1) monitorowanie utrzymania środków trwałych, wartości niematerialnych i prawnych oraz usług nabytych w ramach projektu, w tym ich sprawności technicznej, dostępności oraz przydatności do realizacji założonych celów;
- 2) sprawowanie nadzoru nad prawidłowym i zgodnym z przeznaczeniem użytkowaniem systemów, urządzeń oraz innych zasobów objętych projektem;
- 3) monitorowanie zgodności podejmowanych działań z celami projektu oraz osiągniętymi wskaźnikami określonymi w dokumentacji projektowej;
- 4) identyfikowanie, analizowanie oraz monitorowanie nieprawidłowości i potencjalnych zagrożeń mogących wpływać na trwałość projektu, a także inicjowanie i wdrażanie działań korygujących lub zapobiegawczych.

3. Okres obowiązywania procedury

Procedura obowiązuje przez okres 2 lat od dnia zakończenia realizacji projektu, rozumianego jako dzień zaakceptowania przez Operatora końcowego rozliczenia projektu.

4. Odpowiedzialność

- 1) *Kierownik Jednostki (Starosta Tomaszowski)* odpowiada za:

- a) zapewnienie środków organizacyjnych, technicznych i finansowych niezbędnych do utrzymania efektów projektu;
- b) zatwierdzanie działań naprawczych i doskonalących wynikających z przeprowadzonych przeglądów, audytów oraz raportów;
- c) zatwierdzenie raportu monitorowania utrzymania efektów projektu.

- 2) *Koordynator projektu (Wydział Funduszy Pomocowych, Strategii, Rozwoju i Inwestycji)* odpowiada za:

- a) organizację i koordynację procesu monitorowania utrzymania efektów projektu;

- b) gromadzenie danych i informacji niezbędnych do oceny trwałości projektu;
 - c) przygotowywanie raportów monitorowania utrzymania efektów projektu;
 - d) inicjowanie działań korygujących i doskonalących;
 - e) informowanie Kierownika Jednostki oraz Operatora o ryzykach mogących mieć wpływ na utrzymanie efektów projektu.
- 3) *Informatycy (Referat Administrowania Danymi Osobowymi i Informatyki)* odpowiadają za:
- a) bieżące monitorowanie stanu technicznego urządzeń, systemów i usług objętych projektem;
 - b) kontrolę prawidłowego funkcjonowania systemów wdrożonych w ramach projektu;
 - c) zgłaszanie stwierdzonych nieprawidłowości oraz rekomendowanie działań naprawczych.
- 4) *Pracownicy Jednostki* odpowiadają za:
- a) przestrzeganie obowiązujących procedur, polityk i zasad bezpieczeństwa informacji;
 - b) niezwłoczne zgłaszanie incydentów, awarii oraz innych nieprawidłowości mogących mieć wpływ na utrzymanie efektów projektu;
 - c) współpracę przy realizacji działań monitorujących oraz audytowych związanych z trwałością projektu.

5. Przedmiot monitorowania

Monitorowaniu podlegają w szczególności:

- 1) sprzęt informatyczny zakupiony, zmodernizowany lub wdrożony w ramach projektu;
- 2) oprogramowanie systemowe, użytkowe oraz narzędzia służące zapewnieniu cyberbezpieczeństwa;
- 3) systemy monitorowania, wykrywania, analizowania i rejestrowania zagrożeń oraz incydentów bezpieczeństwa;
- 4) dokumentacja bezpieczeństwa informacji, w szczególności polityki, procedury, instrukcje, plany, ewidencje i rejestry;
- 5) procedury zarządzania incydentami bezpieczeństwa informacji oraz zapewnienia ciągłości działania;
- 6) kompetencje, kwalifikacje oraz poziom świadomości pracowników w zakresie cyberbezpieczeństwa, w tym udział w szkoleniach i działaniach podnoszących świadomość bezpieczeństwa;
- 7) utrzymanie trwałości rezultatów projektu, w tym osiągniętych wskaźników, przez okres wymagany umową o powierzenie grantu oraz obowiązującymi wytycznymi.

6. Sposób monitorowania

- 1) Monitoring techniczny prowadzony jest na bieżąco przez *Informatyków (Referat Administrowania Danymi Osobowymi i Informatyki)* i obejmuje w szczególności:
 - a) kontrolę dostępności oraz poprawności funkcjonowania systemów i usług objętych projektem;
 - b) weryfikację aktualności systemów operacyjnych, aplikacji oraz mechanizmów bezpieczeństwa;
 - c) monitorowanie oraz rejestrowanie incydentów bezpieczeństwa i zdarzeń mogących wpływać na cyberbezpieczeństwo Jednostki.

- 2) Przeglądy okresowe prowadzone są przez *Informatyków (Referat Administrowania Danyimi Osobowymi i Informatyki)* nie rzadziej niż raz na kwartał i obejmują:
 - a) ocenę skuteczności zastosowanych zabezpieczeń technicznych i organizacyjnych;
 - b) weryfikację zgodności konfiguracji systemów i urządzeń z obowiązującymi standardami oraz przyjętymi procedurami;
 - c) analizę zgłoszonych incydentów bezpieczeństwa oraz podjętych działań naprawczych;
 - d) ocenę stopnia realizacji zaleceń wynikających z poprzednich przeglądów, audytów lub kontroli.
- 3) Audyt wewnętrzny przeprowadzany jest przez *Inspektora Ochrony Danych (IOD)*, nie rzadziej niż raz w roku i obejmuje:
 - a) ocenę zgodności działań z obowiązującymi procedurami cyberbezpieczeństwa oraz bezpieczeństwa informacji;
 - b) ocenę realizacji wymagań wynikających z projektu „Cyberbezpieczny Samorząd”;
 - c) identyfikację ryzyk oraz obszarów wymagających działań korygujących lub doskonalących;
 - d) ocenę skuteczności działań podejmowanych w celu utrzymania efektów projektu.
- 4) Wszystkie czynności związane z monitoringiem technicznym, przeglądami okresowymi oraz audytem wewnętrznym podlegają obowiązkowemu udokumentowaniu. Dokumentacja obejmuje w szczególności:
 - a) protokoły z przeglądów okresowych;
 - b) raporty z monitoringu technicznego;
 - c) raporty z audytu wewnętrznego;
 - d) notatki służbowe lub karty kontroli (w przypadku czynności bieżących);
 - e) rejestry incydentów oraz podjętych działań korygujących.
- 5) Wyniki monitoringu technicznego, przeglądów okresowych oraz audytów wewnętrznych stanowią podstawę do oceny utrzymania efektów projektu oraz podejmowania działań korygujących i doskonalących.

7. Wskaźniki oceny utrzymania efektów projektu

Do oceny utrzymania efektów projektu „Cyberbezpieczny Samorząd” stosuje się następujące wskaźniki rezultatu:

- 1) liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym, z podziałem na kobiety i mężczyzn;
- 2) liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym, z podziałem na kobiety i mężczyzn;
- 3) liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji;
- 4) użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych;
- 5) liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST.

8. Sprawozdawczość i archiwizacja

- 1) *Koordinator projektu (Wydział Funduszy Pomocowych, Strategii, Rozwoju i Inwestycji)* sporządza roczny raport monitorowania utrzymania efektów projektu „Cyberbezpieczny Samorząd” przez okres co najmniej 2 lat od dnia zakończenia realizacji projektu.

- 2) Dane i informacje niezbędne do sporządzenia raportów monitorowania utrzymania efektów projektu są zbierane cyklicznie, raz w roku, w I kwartale. Osoby przekazujące dane i informacje na potrzeby sporządzenia raportu są zobowiązane do udzielania wszelkich wyjaśnień oraz przekazywania informacji dotyczących osiągniętych wskaźników *Koordinatorowi projektu (Wydziałowi Funduszy Pomocowych, Strategii, Rozwoju i Inwestycji)*, a także - na żądanie - Operatorowi, Grantodawcy lub Instytucji Zarządzającej FERC.
- 3) Dokumentację monitoringu stanowi raport sporządzony zgodnie z wzorem stanowiącym załącznik nr 1 do niniejszej procedury oraz oświadczenie o wykorzystaniu sprzętu/oprogramowania zgodnie z przeznaczeniem, stanowiące załącznik nr 2 do niniejszej procedury.
- 4) Dokumentacja związana z monitorowaniem utrzymania efektów projektu jest przechowywana w Starostwie Powiatowym w Tomaszowie Mazowieckim, ul. Św. Antoniego 41, 97-200 Tomaszów Mazowiecki, przez okres co najmniej 5 lat od dnia zakończenia realizacji projektu.

9. Postępowanie w przypadku zagrożenia utrzymania efektów

W przypadku wystąpienia ryzyka związanego z utrzymaniem efektów projektu, *Koordinator projektu (Wydział Funduszy Pomocowych, Strategii, Rozwoju i Inwestycji)* niezwłocznie informuje *Kierownika Jednostki (Starostę Tomaszowskiego)* oraz Operatora, zgodnie z § 13 ust. 2 Umowy o powierzenie grantu. Jednocześnie podejmowane są odpowiednie działania naprawcze mające na celu ograniczenie skutków zidentyfikowanego ryzyka oraz zapewnienie utrzymania efektów projektu. Z przebiegu zdarzenia sporządzany jest raport wyjaśniający, zawierający opis zaistniałej sytuacji, podjęte działania oraz ich rezultaty.

10. Postanowienia końcowe

Niniejsza procedura obowiązuje przez cały okres trwałości projektu i podlega przeglądowi oraz aktualizacji w przypadku wystąpienia zmian organizacyjnych, prawnych lub technicznych mających wpływ na realizację jej postanowień lub utrzymanie efektów projektu.



Załącznik nr 1
do Procedury monitorowania
utrzymania efektów projektu
„Cyberbezpieczny Samorząd”

Formularz rocznego raportu monitorowania utrzymania efektów projektu
„Cyberbezpieczny Samorząd”

I. Dane podstawowe

1.	Nazwa jednostki	
2.	Rok sprawozdawczy	
3.	Okres objęty raportem	
4.	Data sporządzenia raportu	

II. Cel raportu

Raport sporządzono w celu oceny utrzymania efektów osiągniętych w ramach projektu „Cyberbezpieczny Samorząd” oraz określenia stopnia funkcjonowania wdrożonych rozwiązań organizacyjnych, kompetencyjnych i technicznych w zakresie cyberbezpieczeństwa.

III. Wskaźniki utrzymania efektów projektu

Lp.	Nazwa wskaźnika rezultatu	Jednostka miary	Wartość osiągnięta zgodnie z końcowym rozliczeniem projektu	Rok osiągnięcia	Stan obecny (utrzymany/zmodyfikowany)
1.	Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (Kobiety)	Szt.			
2.	Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (Mężczyźni)	Szt.			
3.	Liczba pracowników podmiotów wykonujących zadania publiczne nie będących	Szt.			



	pracownikami IT, objętych wsparciem szkoleniowym (Kobiety)				
4.	Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym (Mężczyźni)	Szt.			
5.	Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji	Szt.			

Uzasadnienie (w przypadku zmodyfikowania któregośkolwiek ze wskaźników)

.....
.....
.....

.....
miejscowość i data

.....
podpis osoby uprawnionej



**Załącznik nr 2
do Procedury monitorowania
utrzymania efektów projektu
„Cyberbezpieczny Samorząd”**

**Informatycy
(Referat Administrowania
Danymi Osobowymi
i Informatyki)
Starostwo Powiatowe
w Tomaszowie Mazowieckim
ul. Św. Antoniego 41
97-200 Tomaszów Mazowiecki**

**Koordynator projektu
(Wydział Funduszy Pomocowych,
Strategii, Rozwoju i Inwestycji)
Starostwo Powiatowe
w Tomaszowie Mazowieckim
ul. Św. Antoniego 41
97-200 Tomaszów Mazowiecki**

OŚWIADCZENIE

Oświadczam, że sprzęt oraz oprogramowanie zakupione w ramach projektu grantowego pn. „Cyberbezpieczny Samorząd”, realizowanego w ramach konkursu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Priorytet II: Zaawansowane usługi cyfrowe, Program Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), na podstawie § 13 ust. 1 Umowy o powierzenie grantu o numerze **FERC.02.02-CS.01-001/23/1383/ FERC.02.02-CS.01-001/23/2024**, jest użytkowane zgodnie z założeniami ww. projektu.

Sprzęt i oprogramowanie są utrzymywane w należyтым stanie technicznym, oznakowane zgodnie z wymogami projektu oraz wykorzystywane zgodnie z ich przeznaczeniem.

Jednocześnie oświadczam, że ww. sprzęt i oprogramowanie nie zostały sprzedane, oddane w użyczenie ani w inny sposób przekazane do użytkowania podmiotom trzecim.

.....
miejscowość i data

.....
podpis osoby uprawnionej