

**Załącznik
do Zarządzenia Nr 93/2026
Starosty Kraśnickiego
z dnia 24 września 2026 r.**

**PROCEDURA MONITOROWANIA UTRZYMANIA EFEKTÓW PROJEKTU GRANTOWEGO
„Wzmocnienie poziomu cyberbezpieczeństwa w Powiecie”**

§ 1

Procedura dotyczy utrzymania środków trwałych i usług nabytych w ramach projektu nr FERC.02.02-CS.01-001/23, pn. „Wzmocnienie poziomu cyberbezpieczeństwa w Powiecie” (Umowa o powierzenie grantu nr FERC.02.02-CS.01-001/23/0980/ FERC.02.02-CS.01-001/23/2024 z dnia 19.07.2024 r.) realizowanego w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), priorytet II: Zaawansowane usługi cyfrowe, działanie 2.2 - Wzmocnienie krajowego systemu cyberbezpieczeństwa. Procedura została opracowana zgodnie z § 3 ust. 3, § 7–8 oraz § 13 Umowy.

§ 2

Celem procedury jest zapewnienie trwałości i właściwego wykorzystania efektów projektu, w tym utrzymania przez okres co najmniej **2 lat od zakończenia projektu** nabytych w jego ramach środków trwałych, oprogramowania, usług oraz rezultatów miękkich (szkoleń, podniesienia kompetencji pracowników), których efekt trwały polega na wykorzystaniu zdobytej wiedzy w pracy zawodowej, bez konieczności ponoszenia dodatkowych kosztów szkoleniowych w okresie trwałości.

§ 3

Zakres rzeczowy monitorowania:

1. Monitorowaniu podlegają wszystkie działania i efekty zrealizowane w ramach projektu, uszczegółowione w wykazie elementów podlegających utrzymaniu, tj.:
 - 1) Obszar organizacyjny – wdrożenie i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), procedury i polityki cyberbezpieczeństwa - utrzymanie opracowanych i wdrożonych w ramach projektu dokumentów Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym polityk, procedur, instrukcji i regulacji dotyczących cyberbezpieczeństwa. Utrzymanie oznacza obowiązywanie i praktyczne stosowanie tych dokumentów w działalności urzędu przez cały okres trwałości projektu, bez konieczności ponoszenia dodatkowych kosztów na ich ponowne opracowanie lub aktualizację, o ile nie wynika to bezpośrednio ze zmian przepisów prawa lub struktury organizacyjnej Powiatu. Efektem trwałym jest zachowanie funkcjonalności i skuteczności wdrożonych zasad bezpieczeństwa informacji.
 - 2) Obszar kompetencyjny – przeprowadzone szkolenia dla pracowników urzędu i kadry IT w zakresie cyberbezpieczeństwa, których efekt trwały polega na wykorzystaniu zdobytej wiedzy w pracy zawodowej, bez konieczności ponoszenia dodatkowych kosztów szkoleniowych w okresie trwałości.

- 3) Obszar techniczny – zakupione, zainstalowane i utrzymywane rozwiązania techniczne (m.in. serwer, macierz dyskowa, switchy zarządzalne, systemy operacyjne - wykaz w tabeli formularza monitorowania utrzymania efektów projektu grantowego).

§ 4

Obowiązki Grantobiorcy:

1. Zapewnienie utrzymania w należytym stanie technicznym i organizacyjnym zakupionych środków trwałych i usług.
2. Wykorzystywanie zakupionych systemów, oprogramowania i infrastruktury zgodnie z przeznaczeniem.
3. Przechowywanie dokumentacji związanej z realizacją i utrzymaniem efektów projektu w Wydziale Organizacyjnym.
4. Prowadzenie ewidencji środków trwałych oraz wartości niematerialnych i prawnych nabytych w ramach projektu.
5. Składanie informacji i oświadczeń wymaganych przez Grantodawcę/Operatora w zakresie utrzymania efektów, osiągnięcia wskaźników oraz przestrzegania zasad równościowych i horyzontalnych.

§ 5

1. Efekty projektu będą monitorowane przez okres **2 lat od dnia zatwierdzenia końcowego wniosku rozliczającego projekt**. Protokoły odbioru etapów stanowią dokumentację potwierdzającą prawidłową realizację zakresu i wskazują moment rozpoczęcia utrzymania dla dostarczonych elementów.
2. W tym czasie Grantobiorca zobowiązany jest do:
 - 1) przechowywania zakupionych urządzeń i oprogramowania,
 - 2) odnawiania niezbędnych subskrypcji/aktualizacji,
 - 3) zapewnienia dostępności i funkcjonalności wdrożonych systemów,
 - 4) utrzymania kompetencji kadry poprzez wykorzystanie wiedzy zdobytej podczas szkoleń zrealizowanych w ramach projektu; nie jest wymagane powtarzanie szkoleń ani finansowanie nowych w okresie trwałości.

§ 6

Sposoby monitorowania:

1. **Raportowanie** – składanie okresowych informacji o utrzymaniu efektów na żądanie Grantodawcy/Operatora (zgodnie z §7 ust. 5 Umowy).
2. **Oświadczenia** – przygotowywanie oświadczeń Grantobiorcy o zachowaniu trwałości projektu.
3. **Kontrole** – umożliwienie przeprowadzenia kontroli, audytów i ewaluacji prowadzonych przez Operatora, Grantodawcę, Instytucję Zarządzającą FERC lub inne uprawnione podmioty.
4. **Ewaluacja** – udział w ankietach, wywiadach i badaniach ewaluacyjnych (§8 Umowy).

§ 7

Sankcje za niedotrzymanie warunków:

1. W przypadku stwierdzenia naruszeń w zakresie utrzymania efektów projektu, Grantodawca może żądać zwrotu części lub całości otrzymanego dofinansowania (§5 ust. 6–8 Umowy).

2. Grantobiorca ponosi pełną odpowiedzialność za szkody powstałe w wyniku niewłaściwego wykorzystania sprzętu lub usług zakupionych w ramach projektu.

§ 8

Przechowywanie dokumentacji i wskaźników:

1. Dokumentacja związana z realizacją i utrzymaniem efektów projektu, obejmuje również ewidencję środków trwałych i WNiP wraz z numerami inwentarzowymi/ewidencyjnymi nadanymi zgodnie z zasadami rachunkowości, w tym dokumenty dotyczące wskaźników osiągniętych w ramach projektu, także zatwierdzone dokumenty SZBI (procedury, polityki i regulacje), które będą przechowywane w wersji papierowej lub elektronicznej przez okres 5 lat od zakończenia realizacji projektu lub dłużej, jeśli wymaga tego prawo lub zasady archiwizacji obowiązujące w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027.
2. Wskaźniki dotyczące osiągnięcia celów projektu będą monitorowane i udokumentowane przez okres co najmniej 2 lata od zakończenia realizacji projektu, w celu zapewnienia trwałości efektów oraz realizacji celów projektu zgodnie z wymaganiami Grantodawcy.

§ 9

Postanowienia końcowe

Procedura obowiązuje od dnia zakończenia realizacji projektu do upływu 2 lat od jego zatwierdzonego rozliczenia.

ZAŁĄCZNIK DO PROCEDURY MONITOROWANIA

FORMULARZ MONITOROWANIA UTRZYMANIA

EFEKTÓW PROJEKTU GRANTOWEGO¹

Nazwa projektu Wzmocnienie poziomu cyberbezpieczeństwa w Powiecie
Nr umowy o powierzenie grantu FERC.02.02-CS.01-001/23/0980/ FERC.02.02-CS.01-001/23/2024
Okres sprawozdawczy od.....do.....
Jednostka realizująca Powiat Kraśnicki, Al. Niepodległości 20, 23-204 Kraśnik
Osoba sporządzająca
Stanowisko

I. SPRZĘT I OPROGRAMOWANIE NABYTE W RAMACH PROJEKTU

Lp.	Nazwa środka trwałego / usługi	Producent / Specyfikacja / Nr licencji	Data zakupu	Jednostka / komórka/os. odpowiedzialna za utrzymanie	Nr inw/ewid	Status utrzymania	Uwagi
1.	Przełącznik sieciowy typ 1	Zanonimizowano ze względu na bezpieczeństwo teleinformatyczne infrastruktury urzędu.	27.05.2026r.	Wydział Organizacyjny/informatyk		działa	
2.	Przełącznik sieciowy typ 1		27.05.2026r.	Wydział Organizacyjny/informatyk		działa	
3.	Przełącznik sieciowy typ 1		27.05.2026r.	Wydział Organizacyjny/informatyk		działa	
4.	Przełącznik sieciowy typ 1		27.05.2026r.	Wydział Organizacyjny/informatyk		działa	
5.	Przełącznik sieciowy typ 2		27.05.2026r.	Wydział Organizacyjny/informatyk		działa	
6.	Przełącznik sieciowy typ 2		27.05.2026r.	Wydział Organizacyjny/informatyk		działa	
7.	Zapora sieciowa (firewall)		27.05.2026r.	Wydział Organizacyjny/informatyk		działa	
8.	Zapora sieciowa (firewall)		27.05.2026r.	Wydział Organizacyjny/informatyk		działa	
9.	Serwer z sys. operacyjnym		29.07.2026r.	Wydział Organizacyjny/informatyk		Działa/aktywny	
10.	Macierz dyskowa		29.07.2026r.	Wydział Organizacyjny/informatyk		działa	
11.	System operacyjny		29.07.2026r.	Wydział Organizacyjny/informatyk		aktywny	

**II. SZKOLENIA ZREALIZOWANE W RAMACH PROJEKTU**

Lp.	Nazwa szkolenia	Data realizacji	Liczba uczestników	Jednostka /komórka	Jednostka / komórka/os. odpowiedzialna za utrzymanie	Zakres tematyczny	Status utrzymania	Uwagi
1.	Szkolenie z zakresu cyberbezpieczeństwa dedykowane pracownikom biurowym (os. nietechniczne)	18.09.2026	24	Wszystkie wydziały	Wydział Kadrowy	Podstawy prawne krajowego systemu cyberbezpieczeństwa, obowiązki jednostki samorządu wynikające z ustawy o krajowym systemie cyberbezpieczeństwa, phishing/spoofing ochrona danych, bezpieczne hasła, socjotechniki – podstawowe definicje i przykłady użycia, zagrożenia związane z nieznanym sprzętem usb.	Utrzymano liczbę przeszkolonych osób	
2.	Szkolenie specjalistyczne z zakresu cyberbezpieczeństwa dedykowane pracownikom (administratorom) IT	16.09.2026	2	Wydział Organizacyjny/informatyk	Wydział Kadrowy	Identyfikacja incydentów komputerowych, Zabezpieczenie urządzeń końcowych i użytkownika, wymogi prawne SZBI, audyt systemów IT, Projektowanie mechanizmów kontrolnych bezpieczeństwa systemu.	Utrzymano liczbę przeszkolonych osób	

III. DOKUMENTACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)

W ramach projektu opracowano i wdrożono dokumentację SZBI, obejmującą m.in.:

- Politykę Bezpieczeństwa Informacji,
- Księgę SZBI (podręcznik systemu),
- Procedury SZBI (m.in. incydenty, kopie zapasowe, kontrola dostępu, uprawnienia, ciągłość działania, audyty, zasady ochrony danych i zarządzania infrastrukturą IT),
- Instrukcje, rejestry i formularze (np. rejestr incydentów, rejestr ryzyka),
- Dokumentacja jest obowiązująca i stosowana w organizacji. Aktualizacje mogą być wykonywane wyłącznie w przypadku zmian przepisów prawa lub struktury organizacyjnej, bez konieczności ponoszenia nowych kosztów.

Jednostka / komórka/os. odpowiedzialna za utrzymanie :pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

IV. WSKAŹNIKI PROJEKTU

Wskaźnik	Jednostka	Rok bazowy	Rok realizacji	Wartość
Liczba pracowników IT objętych szkoleniem (kobiety)	szt.	2023	2026	0



Liczba pracowników IT objętych szkoleniem (mężczyźni)	szt.	2023	2026	2
Liczba pracowników nie-IT objętych szkoleniem (kobiety)	szt.	2023	2026	19
Liczba pracowników nie-IT objętych szkoleniem (mężczyźni)	szt.	2023	2026	5
Liczba systemów zwiększających poziom bezpieczeństwa informacji	szt.	2023	2026	4
Użytkownicy nowych i zmodernizowanych usług cyfrowych	szt.	2023	2026	142
Liczba podmiotów JST objętych wsparciem w zakresie cyberbezpieczeństwa	szt.	2023	2026	1

Łączna liczba uczestników szkoleń: **26 osób (2 pracowników IT (0 kobiet i 2 mężczyzn) + 24 pracowników administracyjnych(19 kobiet i 5 mężczyzn))** łącznie **19 kobiet i 7 mężczyzn**.

V. OŚWIADCZENIE O UTRZYMANIU EFEKTÓW PROJEKTU

Ja, niżej podpisany/a, działając w imieniu i na rzecz Powiatu Kraśnickiego, oświadczam, że:

1. Efekty projektu „**Wzmocnienie poziomu cyberbezpieczeństwa w Powiecie**” są utrzymywane zgodnie z umową o powierzenie grantu.
2. Sprzęt, oprogramowanie, systemy i usługi są wykorzystywane zgodnie z przeznaczeniem, utrzymywane w należytym stanie technicznym i eksploatacyjnym.
3. Dokumentacja SZBI jest stosowana i utrzymywana w aktualności.
4. Pracownicy wykorzystują w pracy zawodowej wiedzę zdobytą podczas szkoleń; Efekt szkoleniowy został osiągnięty i jest utrzymywany poprzez stosowanie w pracy wiedzy zdobytej podczas szkoleń, bez konieczności ponoszenia nowych kosztów szkoleniowych.
5. Wskaźniki projektu zostały osiągnięte i są utrzymywane.
6. Dokumentacja potwierdzająca utrzymanie efektów projektu jest przechowywana zgodnie z zasadami archiwizacji i udostępniana na żądanie Grantodawcy lub Operatora.

Oświadczam, że Powiat Kraśnicki utrzymuje powyższe efekty przez okres **24 miesięcy od dnia zakończenia projektu**.

Data sporządzenia:

Podpis osoby sporządzającej:

Podpis Starosty / osoby upoważnionej:

¹ Formularz stanowi podstawę do okresowego raportowania utrzymania efektów projektu oraz może być przekazywany Grantodawcy lub Operatorowi w ramach monitoringu trwałości projektu.