

**Zarządzenie Nr 550/2026
Prezydenta Miasta Kalisza
z dnia 28 września 2026 r.**

w sprawie wprowadzenia „Procedury monitorowania utrzymania efektów oraz trwałości projektu pn. „Zwiększenie cyberbezpieczeństwa w jednostkach Miasta Kalisza”, realizowanego w ramach projektu grantowego „Cyberbezpieczny Samorząd”.

Na podstawie art. 30 ust. 1 i art. 33 ust. 1, 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2026 r. poz. 662 z późn. zm.), zarządza się, co następuje:

§ 1.

Wprowadza się „Procedurę monitorowania utrzymania efektów oraz trwałości projektu pn. „Zwiększenie cyberbezpieczeństwa w jednostkach Miasta Kalisza”, realizowanego w ramach projektu grantowego „Cyberbezpieczny Samorząd”, stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Wykonanie zarządzenia powierza się Sekretarzowi Miasta Kalisza, Dyrektorowi Ośrodka Sportu, Rehabilitacji i Rekreacji w Kaliszu, Dyrektorowi Zarządu Dróg Miejskich w Kaliszu, Dyrektorowi Miejskiego Ośrodka Pomocy Społecznej, przy udziale Skarbnika Miasta Kalisza

§ 3.

Zarządzenie podlega publikacji w Biuletynie Informacji Publicznej.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Kalisza
/.../
Krystian Kinastowski



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik
do zarządzenia Nr 550/2026
Prezydenta Miasta Kalisza
z dnia 28 września 2026 r.

PROCEDURA
monitorowania utrzymania efektów oraz trwałości projektu
pn. „Zwiększenie cyberbezpieczeństwa w jednostkach Miasta Kalisza”,
realizowanego w ramach projektu grantowego „Cyberbezpieczny Samorząd”.

§ 1.

Cel i zakres procedury

1. Niniejsza Procedura monitorowania utrzymania efektów oraz trwałości projektu pn. „Zwiększenie cyberbezpieczeństwa w jednostkach Miasta Kalisza”, realizowanego w ramach projektu grantowego „Cyberbezpieczny Samorząd”.Projektu (zwana dalej „Procedurą”) została opracowana w związku z realizacją przez Miasto Kalisz projektu grantowego pn. „Zwiększenie cyberbezpieczeństwa w jednostkach Miasta Kalisza”, realizowanego w ramach projektu grantowego „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, finansowanego z Europejskiego Funduszu Rozwoju Regionalnego (EFRR) - umową o powierzenie grantu o numerze nr FERC.02.02-CS.01-001/23/0843/FERC.02.02-CS.01-001/23/2024
2. Celem Procedury jest zapewnienie prawidłowego monitorowania utrzymania efektów Projektu, przez okres min. 2 lat od zakończenia projektu zgodnie z zawartą umową o powierzenie grantu o numerze nr FERC.02.02-CS.01-001/23/0843/FERC.02.02-CS.01-001/23/2024. Za datę zakończenia projektu grantowego uważa się datę zaakceptowania przez Operatora końcowego rozliczenia projektu grantowego realizowanego zgodnie z zawartą umową o powierzenie grantu.
3. Procedura obejmuje wszystkie cztery jednostki organizacyjne Miasta Kalisza uczestniczące w Projekcie, które zostały wskazane we wniosku o dofinansowanie jako beneficjenci działań projektowych:
 - 1) Urząd Miasta Kalisza (zwany dalej „UMK”),
 - 2) Zarząd Dróg Miejskich w Kaliszu (zwany dalej „ZDM”),
 - 3) Miejski Ośrodek Pomocy Społecznej w Kaliszu (zwany dalej „MOPS”),
 - 4) Ośrodek Sportu, Rehabilitacji i Rekreacji w Kaliszu (zwany dalej „OSRiR”).
4. Procedura stanowi integralną część systemu zarządzania Projektem i jest wiążąca dla wszystkich osób i jednostek zaangażowanych w utrzymanie efektów Projektu.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

§ 2. Definicje

Użyte w Procedurze pojęcia oznaczają:

- 1) **Projekt** – projekt grantowy pn. „Zwiększenie cyberbezpieczeństwa w jednostkach Miasta Kalisza” realizowany w ramach programu „Cyberbezpieczny Samorząd”, nr naboru FERC.02.02-CS.01-001/23.
- 2) **Grantobiorca** – Miasto Kalisz z siedzibą przy ul. Główny Rynek 20, 62-800 Kalisz, NIP 6180015933, REGON 250855877, będące beneficjentem dofinansowania w ramach Projektu.
- 3) **Efekty Projektu** – zakupiony sprzęt, wdrożone oprogramowanie, przeprowadzone szkolenia oraz usługi nabyte w ramach Projektu w zakresie trzech zadań: Zadania 1 (technicznego – zakup sprzętu i oprogramowania), Zadania 2 (kompetencyjnego – podniesienie kompetencji pracowników) oraz Zadania 3 (organizacyjnego – przegląd i doskonalenie systemu zarządzania bezpieczeństwem informacji). Efekty Projektu obejmują wszystkie składniki majątkowe, niematerialne i prawne oraz rezultaty działań szkoleniowych i audytowych, które zostały osiągnięte w wyniku realizacji Projektu.
- 4) **Utrzymanie efektów Projektu** – poprawne i ciągle użytkowanie usług, sprzętu i oprogramowania zgodnie z przeznaczeniem określonym w dokumentacji projektowej, prowadzenie konserwacji i przeglądów technicznych zgodnie z zaleceniami producentów, dokonywanie niezbędnych napraw i wymiany komponentów w celu zachowania pełnej funkcjonalności, niedopuszczanie do sprzedaży, oddania w dzierżawę, przekazania lub innego zbycia sprzętu i oprogramowania na rzecz osób trzecich, a także utrzymanie kompetencji pracowników przeszkolonych w ramach Projektu oraz przestrzeganie zaktualizowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
- 5) **Koordynator** - pracownik Wydziału Organizacyjnego Urzędu Miasta Kalisza wyznaczony przez Sekretarza Miasta Kalisza do koordynowania monitorowania efektów Projektu – odpowiedzialny za koordynację monitorowania na poziomie Grantobiorcy, nadzór nad realizacją Procedury.
- 6) **Roczny Raport z Monitorowania** – dokument sporządzany co 12 miesięcy przez Koordynatora , dokumentujący stan utrzymania efektów Projektu we wszystkich czterech jednostkach uczestniczących w Projekcie.
- 7) **Administrator IT** – osoba wyznaczona w każdej z jednostek uczestniczących w Projekcie (UMK, ZDM, MOPS, OSRiR), odpowiedzialna za bieżące użytkowanie, konserwację i monitoring zakupionego sprzętu i oprogramowania w swojej jednostce oraz za raportowanie stanu do Koordynatora.
- 8) **SZBI (System Zarządzania Bezpieczeństwem Informacji)** – zbiór polityk, procedur, planów i regulacji wewnętrznych dotyczących zarządzania bezpieczeństwem informacji w UMK i OSRiR, który został poddany przeglądowi i aktualizacji w ramach Projektu.
- 9) **Incydent bezpieczeństwa** – każde zdarzenie mogące wpłynąć na poufność, integralność lub dostępność danych i systemów informatycznych w jednostkach objętych Projektem, w tym awarie sprzętu, ataki cybernetyczne, naruszenia procedur bezpieczeństwa, utrata lub kradzież sprzętu.



10) **Operator** – Naukowa i Akademicka Sieć Komputerowa.

§ 3.

Osoby odpowiedzialne

1. **Koordinator** odpowiada za:

- 1) ogólny nadzór nad realizacją Procedury we wszystkich jednostkach uczestniczących w Projekcie,
- 2) zbieranie, weryfikację i konsolidację informacji z poszczególnych jednostek w zakresie utrzymania efektów Projektu,
- 3) sporządzanie Rocznych Raportów z Monitorowania oraz sprawozdania końcowego po zakończeniu okresu trwałości Projektu,
- 4) przechowywanie całości dokumentacji związanej z monitorowaniem, w tym formularzy przeglądów, raportów, protokołów i ewidencji,
- 5) koordynację działań naprawczych w przypadku stwierdzenia nieprawidłowości,
- 6) organizację spotkań z Administratorami IT poszczególnych jednostek w celu omówienia stanu utrzymania efektów Projektu,
- 7) zapewnienie terminowego przekazywania informacji o stanie Projektu do Prezydenta Miasta Kalisza oraz Wydziału Strategii i Rozwoju Urzędu Miasta Kalisza.

2. **Administratorzy IT poszczególnych jednostek** (wyznaczeni w UMK, ZDM, MOPS i OSRiR) odpowiadają za:

- 1) bieżące użytkowanie zakupionego sprzętu i oprogramowania zgodnie z przeznaczeniem określonym w dokumentacji projektowej,
- 2) prowadzenie szczegółowej ewidencji sprzętu i oprogramowania w swojej jednostce, obejmującej numery seryjne urządzeń, daty nabycia, wartości, lokalizacje oraz osoby odpowiedzialne za poszczególne składniki,
- 3) przeprowadzanie regularnych przeglądów technicznych i konserwacji sprzętu zgodnie z zaleceniami producentów oraz harmonogramem określonym w § 5,
- 4) monitorowanie aktywności licencji oprogramowania oraz terminów ich odnowienia,
- 5) raportowanie stanu sprzętu i oprogramowania do Koordynatora z wykorzystaniem formularzy stanowiących Załącznik nr 1 do niniejszej Procedury,
- 6) niezwłoczne informowanie Koordynatora o wszelkich zdarzeniach mogących wpłynąć na utrzymanie efektów Projektu, w szczególności o awariach, incydentach bezpieczeństwa, kradzieżach lub zniszczeniach sprzętu,
- 7) podejmowanie natychmiastowych działań naprawczych w przypadku stwierdzenia nieprawidłowości,
- 8) dokumentowanie wszystkich czynności związanych z konserwacją, naprawami i wymianami komponentów,
- 9) zapewnienie, że sprzęt i oprogramowanie są wykorzystywane wyłącznie do celów związanych z realizacją zadań jednostki w zakresie cyberbezpieczeństwa,
- 10) współpracę z Koordynatorem w zakresie przygotowania dokumentacji do kontroli zewnętrznych.



3. **Kierownicy poszczególnych jednostek** (Dyrektor ZDM, Dyrektor MOPS, Dyrektor OSRiR) odpowiadają za:

- 1) zapewnienie warunków organizacyjnych, technicznych i lokalowych umożliwiających prawidłowe utrzymanie efektów Projektu w swoich jednostkach,
- 2) wyznaczenie Administratora IT odpowiedzialnego za realizację zadań określonych w ust. 2,
- 3) zapewnienie dostępu do środków finansowych niezbędnych do przeprowadzenia konserwacji, napraw i wymiany komponentów,
- 4) nadzór nad przestrzeganiem Procedury przez pracowników jednostki,
- 5) współpracę z Koordynatorem w zakresie monitorowania i raportowania,
- 6) zapewnienie, że pracownicy przeszkoleni w ramach Projektu wykorzystują nabyte kompetencje w bieżącej pracy, a w przypadku zatrudnienia nowych pracowników wyznaczony pracownik IT przeprowadzi instruktaż stanowiskowy z zakresu cyberbezpieczeństwa, bazując na materiałach wypracowanych w Projekcie.
- 7) wdrażanie zaleceń pokontrolnych oraz działań naprawczych wskazanych przez Koordynatora.

4. **Prezydent Miasta Kalisza** jako osoba reprezentująca Grantobiorcę:

- 1) zatwierdza niniejszą Procedurę oraz wszelkie jej zmiany,
- 2) sprawuje ogólny nadzór nad realizacją zobowiązań wynikających z umowy o powierzenie grantu,
- 3) podejmuje decyzje w sprawach istotnych dla utrzymania trwałości Projektu,
- 4) jest informowany przez Koordynatora o wszelkich istotnych zdarzeniach mogących wpłynąć na realizację zobowiązań projektowych.

§ 4.

Zakres monitorowania

Zadanie 1 (techniczne – zakup sprzętu i oprogramowania)

1. **Macierze dyskowe QNAP** (UMK, ZDM, MOPS, OSRiR) - monitorowaniu podlega:
 - 1) sprawność techniczna macierzy i wszystkich zainstalowanych dysków,
 - 2) ciągłość zapisu i odczytu danych,
 - 3) status dysków w macierzy (aktywne, zapasowe, uszkodzone),
 - 4) wykorzystanie pojemności dysków,
 - 5) logi błędów i ostrzeżeń systemowych,
 - 6) stan dysków zapasowych i ich gotowość do użycia,
 - 7) poprawność konfiguracji RAID,
 - 8) wykonywanie kopii zapasowych zgodnie z harmonogramem.
2. **Zasilacze awaryjne Cyber Power** (UMK, ZDM, MOPS, OSRiR) - monitorowaniu podlega:
 - 1) stan akumulatorów (pojemność, wiek, cykle ładowania),
 - 2) czas podtrzymania napięcia w warunkach testowych,
 - 3) logi testów automatycznych i manualnych,
 - 4) sprawność układów ładowania i przełączania,
 - 5) historia zdarzeń (zanimki napięcia, przełączenia na zasilanie awaryjne),



- 6) poprawność konfiguracji oprogramowania zarządzającego UPS,
- 7) wykonywanie testów obciążeniowych zgodnie z zaleceniami producenta.

3. **Oprogramowanie ESET PROTECT ENTRY ON-PREM (UMK)** - monitorowaniu podlega:

- 1) aktywność licencji i termin jej ważności,
- 2) aktualność sygnatur wirusów i definicji zagrożeń,
- 3) liczba chronionych stanowisk (weryfikacja zgodności z licencją na 650 stanowisk),
- 4) logi skanowania i wykrytych zagrożeń,
- 5) poprawność konfiguracji zapory osobistej,
- 6) funkcjonalność modułu anti-theft,
- 7) skuteczność ochrony antyspamowej,
- 8) regularne aktualizacje oprogramowania.

4. **Zapory sieciowe Fortinet FortiGate - modele: 50G, 70G, 200G (UMK, ZDM, MOPS, OSRiR)** - monitorowaniu podlega:

- 1) sprawność urządzenia i wszystkich jego modułów,
- 2) aktywność licencji wsparcia technicznego,
- 3) poprawność konfiguracji,
- 4) przepustowość i wydajność w czasie rzeczywistym,
- 5) logi zablokowanych ataków i zagrożeń,
- 6) statystyki ruchu sieciowego,
- 7) aktualizacje firmware i sygnatur zagrożeń,
- 8) poprawność działania mechanizmów deszyfrowania i szyfrowania pakietów.

5. **Przełączniki sieciowe TP-Link SG3452 (OSRiR)** - monitorowaniu podlega:

- 1) sprawność techniczna wszystkich portów,
- 2) poprawność konfiguracji,
- 3) kontrola ruchu sieciowego i mechanizmów QoS,
- 4) wykorzystanie przepustowości,
- 5) logi błędów i zdarzeń sieciowych,
- 6) aktualizacje firmware,
- 7) poprawność działania mechanizmów kontroli wzrostu natężenia ruchu.

6. **System do kompleksowego zarządzania zasobami IT eAuditor (UMK)** - monitorowaniu podlega:

- 1) aktywność systemu i wszystkich jego modułów,
- 2) liczba monitorowanych stanowisk (weryfikacja zgodności z licencją na 550 stanowisk),
- 3) poprawność działania modułów ochrony (szyfrowanie BitLocker, blokowanie portów USB, monitorowanie sieci),
- 4) logi zablokowanych procesów, stron www i urządzeń,
- 5) statystyki wykrytych zagrożeń,
- 6) aktualność bazy danych urządzeń w sieci,
- 7) poprawność działania wirtualnej mapy sieci,
- 8) wykorzystanie kompetencji przez 4 przeszkolonych pracowników.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

7. Licencja Windows Server 2025 64bit Polish 16 Core (UMK) - monitorowaniu podlega:

- 1) aktywność licencji,
- 2) zgodność z wymogami licencyjnymi.

8. Licencje Windows Server 2025 CAL User (UMK) - monitorowaniu podlega:

- 1) aktywność licencji,
- 2) liczba aktywnych użytkowników,
- 3) zgodność z wymogami licencyjnymi.

9. Usługa wdrożenia i konfiguracji systemu ZABBIX (UMK) - monitorowaniu podlega:

- 1) sprawność systemu ZABBIX i wszystkich jego komponentów,
- 2) aktywność instancji Zabbix Proxy (2 wirtualne maszyny),
- 3) aktywność instancji Grafana,
- 4) zakres monitorowanych urządzeń i sieci,
- 5) poprawność działania wykonanych templates,
- 6) skuteczność wykrywania zagrożeń w oparciu o niskopoziomowe reguły,
- 7) wydajność i dostępność serwera Zabbix,
- 8) logi zdarzeń i powiadomień,
- 9) poprawność monitorowania stron www,
- 10) funkcjonalność pułapek SNMP, IPMI, JMX,
- 11) monitorowanie plików logu.

Zadanie 2 (kompetencyjne – podniesienie kompetencji pracowników)

10. Szkolenia specjalistyczne dla zespołu IT ((UMK, ZDM, MOPS, OSRiR) - monitorowaniu podlega:

- 1) posiadanie certyfikatów ukończenia szkolenia przez przeszkolonych pracowników IT,
- 2) zastosowanie wiedzy w bieżącej pracy,
- 3) zmniejszenie konieczności korzystania ze wsparcia firm zewnętrznych.

11. Szkolenia podstawowe dla pracowników z zakresu cyberbezpieczeństwa (UMK, ZDM, MOPS, OSRiR) - monitorowaniu podlega:

- 1) dokumentacja przeprowadzonych szkoleń (listy obecności, programy szkoleń, materiały szkoleniowe, certyfikaty o ukończeniu szkolenia),
- 2) liczba incydentów cyberbezpieczeństwa wynikających z błędów ludzkich.

Zadanie 3 (organizacyjne – przegląd i doskonalenie systemu zarządzania bezpieczeństwem informacji)

12. Testy socjotechniczne z zakresu cyberbezpieczeństwa (UMK) - monitorowaniu podlega:

- 1) dokumentacja wyników testów socjotechnicznych,
- 2) dokumentacja podjętych działań następczych w odpowiedzi na wyniki testów,
- 3) analiza skuteczności szkoleń w kontekście poprawy reakcji pracowników na zagrożenia.



13. Przegląd oraz aktualizacja dokumentacji SZBI (UMK i OSRiR) - monitorowaniu podlega:

- 1) posiadanie zaktualizowanej dokumentacji SZBI przez UMK i OSRiR,
- 2) obowiązywanie zaktualizowanej dokumentacji (formalne zatwierdzenie przez kierownictwo jednostek),
- 3) przestrzeganie zaktualizowanej dokumentacji przez pracowników,
- 4) realizacja zaleceń wynikających z przeglądu,
- 5) dokumentacja przeprowadzonej analizy ryzyka,
- 6) skuteczność wdrożenia nowych lub zaktualizowanych polityk i procedur.

14. Audyt SZBI (UMK, ZDM, MOPS, OSRiR) - monitorowaniu podlega:

- 1) posiadanie raportu z audytu SZBI,
- 2) realizacja ewentualnych zaleceń poaudytowych,
- 3) dokumentacja działań podjętych w odpowiedzi na zalecenia audytowe,
- 4) terminy realizacji zaleceń,
- 5) poprawa funkcjonowania SZBI w wyniku realizacji zaleceń,
- 6) przeprowadzanie audytów następczych w przypadku istotnych niezgodności.

§ 5.

Harmonogram monitorowania

1. Monitorowanie utrzymania efektów Projektu prowadzone jest przez okres min. 2 lat od zakończenia projektu.
2. Monitorowanie przeprowadzane jest w następującym cyklu:

Etap	Zakres	Odpowiedzialny	Termin	Forma dokumentacji
Przegląd roczny	Szczegółowe sprawdzenie sprawności wszystkich składników sprzętu i oprogramowania nabytych w ramach Projektu (macierze, zapory, UPS, ESET, ZABBIX).	Administratorzy IT poszczególnych jednostek	Do 31 grudnia	Roczny Raport z Monitorowania (Załącznik nr 1 do niniejszej Procedury) w zakresie dotyczącym jednostki
Roczny Raport z Monitorowania	Pełny przegląd wszystkich efektów Projektu	Koordynator na podstawie danych od Administratorów IT	Do 31 stycznia każdego roku za rok poprzedni	Roczny Raport z Monitorowania (Załącznik nr 1 do niniejszej Procedury)
Sprawozdanie końcowe	Podsumowanie całego okresu utrzymania efektów Projektu.	Koordynator	Do 30 dni po upływie 2 lat od zakończenia projektu.	Sprawozdanie końcowe z utrzymania efektów Projektu zatwierdzone przez Prezydenta Miasta Kalisza



3. Koordynator otrzymuje od Administratorów IT poszczególnych jednostek wypełniony formularz Roczno Raportu z Monitorowania (Załącznik nr 1 do niniejszej Procedury) w zakresie dotyczącym ich jednostki.
4. Koordynator konsoliduje informacje z poszczególnych jednostek, weryfikuje ich kompletność i poprawność, sporządza zbiorczy Roczny Raport z Monitorowania i przedkłada go do zatwierdzenia Prezydentowi Miasta Kalisza nie później niż do 31 stycznia każdego roku.
5. W przypadku stwierdzenia istotnych nieprawidłowości wymagających natychmiastowej interwencji, Administratorzy IT informują Koordynatora niezwłocznie, nie czekając na termin przeglądu rocznego.

§ 6.

Sposób dokumentowania

1. Dokumentacja monitorowania obejmuje:
 - 1) wypełnione przez Administratorów IT formularze przeglądów rocznych,
 - 2) Roczne Raporty z Monitorowania zatwierdzone przez Prezydenta Miasta Kalisza,
 - 3) Sprawozdanie końcowe z utrzymania efektów Projektu,
 - 4) ewidencję sprzętu i oprogramowania nabytego w ramach Projektu,
 - 5) kopie certyfikatów i zaświadczeń potwierdzających ukończenie szkoleń specjalistycznych przez pracowników IT,
 - 6) dokumentację szkoleń podstawowych z zakresu Cyberbezpieczeństwa, w tym: listy obecności, certyfikaty o ukończeniu szkolenia, program szkolenia, materiały szkoleniowe,
 - 7) kopie zaktualizowanej dokumentacji SZBI dla UMK i OSRiR po jej przeglądzie i aktualizacji,
 - 8) raporty z audytu SZBI dla wszystkich jednostek (UMK, ZDM, MOPS, OSRiR),
 - 9) dokumentację wyników testów socjotechnicznych przeprowadzonych w UMK,
 - 10) protokoły przeglądów technicznych i konserwacji sprzętu,
 - 11) dokumentację incydentów bezpieczeństwa,
 - 12) dokumentację działań naprawczych podjętych w odpowiedzi na stwierdzone nieprawidłowości.
2. Sprzęt i oprogramowanie przeznaczone zostają do wyłącznego użytku dla uprawnionych pracowników jednostek uczestniczących w Projekcie. Pracownicy zobowiązani są odpowiednio utrzymać, konserwować i używać zgodnie z przeznaczeniem otrzymany sprzęt i oprogramowanie co najmniej przez ustalony okres.
3. Całość dokumentacji monitorowania przechowywana jest w Wydziale Organizacyjnym Urzędu Miasta Kalisza przez okres wymagany przepisami dotyczącymi przechowywania dokumentacji projektów współfinansowanych ze środków Unii Europejskiej. Dokumentacja przechowywana jest w sposób zapewniający jej bezpieczeństwo, poufność i dostępność dla osób uprawnionych.
4. Dokumentacja monitorowania udostępniana jest na każde wezwanie Instytucji Zarządzającej, Grantodawcy lub innych podmiotów uprawnionych do kontroli (w tym organów kontroli finansowej i audytu) w terminie przez nich wskazanym, nie krótszym jednak niż 7 dni roboczych od dnia otrzymania wezwania, chyba że charakter kontroli wymaga udostępnienia dokumentacji w terminie krótszym.



5. Dokumentacja monitorowania może być prowadzona w formie papierowej lub elektronicznej, z zastrzeżeniem, że dokumenty wymagające podpisu (protokoły, raporty, zatwierdzenia) muszą być opatrzone podpisem własnoręcznym lub kwalifikowanym podpisem elektronicznym zgodnie z obowiązującymi przepisami.

§ 7.

Zasady postępowania w przypadku stwierdzenia naruszeń

1. W przypadku stwierdzenia w toku monitorowania jakichkolwiek nieprawidłowości w zakresie utrzymania efektów Projektu, w szczególności:

- 1) awarii sprzętu uniemożliwiającej jego użytkowanie,
- 2) wygaśnięcia licencji oprogramowania,
- 3) utraty lub kradzieży sprzętu,
- 4) zniszczenia sprzętu w wyniku zdarzeń losowych (pożar, zalanie, przepięcie),
- 5) zmiany przeznaczenia sprzętu lub oprogramowania,
- 6) sprzedaży, oddania w dzierżawę lub przekazania sprzętu osobom trzecim,
- 7) naruszenia procedur SZBI,
- 8) incydentu bezpieczeństwa,
- 9) utraty kompetencji przez przeszkolonych pracowników (np. w wyniku ich odejścia z pracy),
- 10) niewykonywania zaleceń poaudytowych,

odpowiednio Administrator IT jednostki lub Koordynator zobowiązani są do:

- 1) niezwłocznego odnotowania zdarzenia w dokumentacji monitorowania z podaniem daty, godziny, okoliczności i skutków zdarzenia,
 - 2) podjęcia natychmiastowych działań zabezpieczających w celu minimalizacji skutków zdarzenia (np. izolacja uszkodzonego sprzętu, tymczasowe rozwiązania zastępcze),
 - 3) przeprowadzenia analizy przyczyn zdarzenia,
 - 4) opracowania planu działań naprawczych z określeniem terminów realizacji i osób odpowiedzialnych,
 - 5) podjęcia działań naprawczych w najkrótszym możliwym terminie, nie dłuższym niż 30 dni od stwierdzenia naruszenia, chyba że charakter naruszenia wymaga dłuższego terminu (np. konieczność przeprowadzenia postępowania o zamówienie publiczne na naprawę lub wymianę sprzętu),
 - 6) powiadomienia Koordynatora (w przypadku jednostek ZDM, MOPS, OSRiR) lub bezpośrednio Prezydenta Miasta Kalisza (w przypadku UMK) – nie później niż w terminie 3 dni roboczych od stwierdzenia naruszenia,
2. W przypadku trwałej utraty możliwości korzystania ze sprzętu lub oprogramowania nabytego w ramach Projektu (np. w wyniku całkowitego zniszczenia, kradzieży bez możliwości odzyskania, nieodwracalnej awarii), Grantobiorca niezwłocznie, nie później niż w terminie 7 dni roboczych od stwierdzenia, informuje o tym fakcie Operatora i podejmuje kroki zgodnie z zapisami umowy o powierzenie grantu.
 3. Działania naprawcze dokumentowane są jako odrębna pozycja w Rocznym Raporcie z Monitorowania.

4. Koordynator prowadzi rejestr naruszeń, w którym odnotowuje wszystkie stwierdzone nieprawidłowości, podjęte działania naprawcze oraz ich skuteczność. Rejestr naruszeń stanowi załącznik do Rocznego Raportu z Monitorowania.

§ 8.

Finansowanie utrzymania efektów Projektu

Koszty utrzymania efektów Projektu, w tym koszty konserwacji, napraw, wymiany komponentów, odnowienia licencji oraz szkoleń uzupełniających, pokrywane są ze środków własnych Grantobiorcy, to jest z budżetu Miasta Kalisza oraz budżetów jednostek uczestniczących w Projekcie.

§ 9.

Szkolenia i podnoszenie kompetencji

1. W celu zapewnienia ciągłości kompetencji nabytych w ramach Projektu, Kierownicy poszczególnych jednostek zobowiązani są do:
 - 1) utrzymania w zatrudnieniu pracowników przeszkolonych w ramach Projektu przez cały okres trwania Projektu, o ile jest to możliwe,
 - 2) w przypadku odejścia z pracy pracownika przeszkolonego w ramach Projektu – zapewnienia przeszkolenia jego następcy w zakresie niezbędnym do kontynuacji zadań związanych z utrzymaniem efektów Projektu,
 - 3) organizacji szkoleń uzupełniających dla pracowników w zakresie nowych zagrożeń cybernetycznych i metod ochrony,
 - 4) zapewnienia pracownikom dostępu do materiałów szkoleniowych, dokumentacji technicznej i źródeł wiedzy niezbędnych do prawidłowego wykonywania zadań.
2. Informacje o szkoleniach uzupełniających oraz o zmianach w składzie osobowym pracowników odpowiedzialnych za utrzymanie efektów Projektu dokumentowane są w Rocznym Raporcie z Monitorowania.

§ 10.

Postanowienia końcowe

1. Procedura wchodzi w życie z dniem jej zatwierdzenia przez Prezydenta Miasta Kalisza i obowiązuje przez okres min. 2 lat od zakończenia projektu zgodnie z zawartą umową o powierzenie grantu o numerze nr FERC.02.02-CS.01-001/23/0843/FERC.02.02-CS.01-001/23/2024. Za datę zakończenia projektu grantowego uważa się datę zaakceptowania przez Operatora końcowego rozliczenia projektu grantowego realizowanego zgodnie z zawartą umową o powierzenie grantu.
2. W sprawach nieuregulowanych niniejszą Procedurą zastosowanie mają w szczególności:
 - 1) zapisy umowy o powierzenie grantu nr FERC.02.02-CS.01-001/23,
 - 2) wytyczne Instytucji Zarządzającej lub Grantodawcy dotyczące realizacji projektów w ramach programu „Cyberbezpieczny Samorząd”,



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

3. Koordynator zapewnia zapoznanie wszystkich osób odpowiedzialnych za realizację Procedury (Administratorów IT, Kierowników jednostek) z jej treścią oraz ze wszelkimi zmianami Procedury. Fakt zapoznania się z Procedurą potwierdzany jest podpisem na liście zapoznania, która stanowi załącznik do dokumentacji Projektu.
4. Integralną część Procedury stanowią następujące załączniki:
 - 1) Załącznik nr 1 – Formularz Roczego Raportu z Monitorowania Utrzymania Efektów Projektu,
 - 2) Załącznik nr 2 – Lista Zapoznania z Procedurą.

Prezydent Miasta Kalisza

/.../

Krystian Kinastowski

Załącznik nr 1 do Procedury

FORMULARZ ROCZNEGO RAPORTU Z MONITOROWANIA UTRZYMANIA EFEKTÓW PROJEKTU

ZADANIE 1 – SPRZĘT I OPROGRAMOWANIE
1. Macierze dyskowe QNAP (wypełnia: UMK, ZDM, MOPS, OSRiR)

Lp.	Składnik majątku	Jednostka	Liczba sztuk	Stan techniczny (sprawny / niesprawny / do naprawy)	Wykorzystanie pojemności (%)	Liczba awarii w okresie sprawozdawczym	Uwagi

Szczegółowe informacje o macierzach dyskowych:

.....

.....

2. Zasilacze awaryjne Cyber Power (wypełnia: UMK, ZDM, MOPS, OSRiR)

Lp.	Składnik majątku	Jednostka	Liczba sztuk	Stan akumulatorów (dobry / wymaga wymiany)	Czas podtrzymania napięcia (min)	Liczba zdarzeń przełączenia na zasilanie awaryjne	Uwagi

Szczegółowe informacje o zasilaczach UPS:

.....

.....

3. Oprogramowanie ESET PROTECT ENTRY (wypełnia: UMK)

Lp.	Składnik majątku	Jednostka	Liczba stanowisk	Aktywność licencji (TAK / NIE)	Termin ważności licencji	Liczba chronionych stanowisk	Uwagi

Szczegółowe informacje o oprogramowaniu:

.....

.....

4. Zapory sieciowe Fortinet FortiGate (modele: 50G, 70G, 200G) (wypełnia: UMK, ZDM, MOPS, OSRiR)

Lp.	Składnik majątku	Jednostka	Liczba sztuk	Stan techniczny	Aktywność licencji wsparcia	Termin ważności licencji	Uwagi

Szczegółowe informacje o zaporach sieciowych:

.....

.....

5. Przełączniki sieciowe TP-Link SG3452 (wypełnia: OSRiR)

Lp.	Składnik majątku	Jednostka	Liczba sztuk	Stan techniczny	Liczba portów sprawnych	Poprawność konfiguracji	Uwagi

Szczegółowe informacje o przełącznikach:

.....

.....

6. System do kompleksowego zarządzania zasobami IT e-Auditor wraz z Licencją Windows Server 2025 64bit Polish 16 Core oraz Licencją Windows Server 2025 CAL User (wypełnia: UMK)

Szczegółowe informacje o systemie:

.....

.....

7. Wdrożenie i konfiguracja systemu ZABBIX (wypełnia: UMK)

Lp.	Element	Jednostka	Status (sprawny / niesprawny)	Zakres monitorowanych urządzeń i sieci	Liczba wykrytych zagrożeń w okresie sprawozdawczym	Uwagi

Szczegółowe informacje o systemie ZABBIX:

.....

.....

**ZADANIE 2 – KOMPETENCJE PRACOWNIKÓW****1. Szkolenia specjalistyczne dla zespołu IT** (wypełnia: UMK, ZDM, MOPS, OSRiR)

Lp.	Rodzaj szkolenia	Jednostka	Liczba przeszkolonych pracowników	Posiadanie certyfikatów / zaświadczeń (TAK / NIE)	Zastosowanie wiedzy w bieżącej pracy (TAK / NIE)	Uwagi

Szczegółowe informacje o szkoleniach specjalistycznych:

.....

.....

2. Szkolenia podstawowe z zakresu Cyberbezpieczeństwa (wypełnia: UMK, ZDM, MOPS, OSRiR)

Lp.	Rodzaj szkolenia	Jednostka	Liczba przeszkolonych pracowników	Posiadanie zaświadczeń (TAK / NIE)	Poprawa świadomości zagrożeń (TAK / NIE)	Uwagi

Szczegółowe informacje o szkoleniach podstawowych:

.....

.....

3. Testy socjotechniczne (wypełnia: UMK)

Lp.	Element	Jednostka	Dokumentacja wyników testów (posiadana / nieposiadana)	Dokumentacja działań następnych (posiadana / nieposiadana)	Uwagi

Szczegółowe informacje o testach socjotechnicznych:

.....

.....

ZADANIE 3 – SZBI I AUDYT

1. Przegląd oraz aktualizacja dokumentacji SZBI (wypełnia: UMK, OSRiR)

Lp.	Element	Jednostka	Zaktualizowana dokumentacja SZBI (posiadana / nieposiadana)	Obowiązywanie dokumentacji (TAK / NIE)	Przestrzeganie dokumentacji (TAK / NIE)	Uwagi

Szczegółowe informacje o dokumentacji SZBI:

.....

.....

2. Audyt SZBI (wypełnia: UMK, ZDM, MOPS, OSRiR)

Lp.	Element	Jednostka	Raport z audytu (posiadany / nieposiadany)	Realizacja zaleceń poaudytowych (TAK / NIE / nie dotyczy)	Uwagi

Szczegółowe informacje o audycie SZBI:

.....

.....

PODSUMOWANIE I STWIERDZONE NIEPRAWIDŁOWOŚCI (wypełnia Koordynator)

1. Ogólna ocena stanu utrzymania efektów Projektu

Obszar	Ocena (dobry / zadowalający / niezadowalający)	Uwagi
Zadanie 1 – Sprzęt i oprogramowanie		
Zadanie 2 – Kompetencje pracowników		
Zadanie 3 – SZBI i audyt		
Ogólna ocena		

2. Stwierdzone nieprawidłowości / zdarzenia / awarie

Lp.	Data stwierdzenia	Rodzaj nieprawidłowości	Jednostka	Opis	Skutki	Przyczyny



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

3. Podjęte działania naprawcze

Lp.	Nieprawidłowość	Opis działań naprawczych	Termin realizacji	Osoba odpowiedzialna	Status realizacji (zrealizowane / w trakcie / niezrealizowane)	Koszty (PLN)	Źródło finansowania

4. Ocena skuteczności działań naprawczych

Prezydent Miasta Kalisza
/.../
Krystian Kinastowski



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik nr 2 do Procedury

Lista Zapoznania z Procedurą.

Niniejszym potwierdzam zapoznanie się z „Procedurą monitorowania utrzymania efektów oraz trwałości projektu pn. „Zwiększenie cyberbezpieczeństwa w jednostkach Miasta Kalisza”, realizowanego w ramach projektu grantowego „Cyberbezpieczny Samorząd” oraz zobowiązuje się do przestrzegania jej zapisów i realizacji wskazanych obowiązków:

L.p.	Imię i Nazwisko	Jednostka organizacyjna	Stanowisko służbowe	Data	Czytelny podpis

Prezydent Miasta Kalisza
/.../
Krystian Kinastowski