# REGULAMIN ROZWOJU APLIKACJI (W ASPEKCIE BEZPIECZEŃSTWA INFORMACJI)

## Spis treści:

## § 1.

## Definicje

Użyte w regulaminie określenia oznaczają:

1) autentyczność – właściwość zapewniającą, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy takich podmiotów jak użytkownicy oraz procesów, systemów i informacji;
2) dokumentacja – kompletny zestaw opisów, rysunków i innych informacji umożliwiających poprawne użytkowanie i eksploatowanie aplikacji;
3) dokumentacja analityczna – kompletny, jednoznaczny i spójny opis wszystkich funkcji aplikacji;
4) infrastruktura teleinformatyczna - środowisko złożone z systemów komputerowych i urządzeń łącznie z systemami operacyjnymi, oprogramowaniem narzędziowym systemu operacyjnego i oprogramowaniem baz danych;
5) kopia zapasowa – duplikat danych, przechowywany na wymiennym nośniku komputerowym, służący do odtworzenia systemu, aplikacji, bazy danych lub dokumentu;
6) modyfikacja – zmianę aplikacji uzyskaną na skutek spełnienia jednego lub kilku warunków, np. zmiany istniejącej funkcjonalności aplikacji lub rozbudowę aplikacji o nową funkcjonalność, bądź zmianę dokumentacji;
7) niezaprzeczalność – możliwość przeprowadzenia dowodu, że działanie lub zdarzenie miało miejsce, tak że nie można temu działaniu lub zdarzeniu później zaprzeczyć;
8) platforma aplikacyjna – umieszczone na infrastrukturze teleinformatycznej oprogramowanie standardowe, z których ARiMR korzysta na podstawie licencji i w oparciu o które wdrożono aplikacje ARiMR;
9) rozliczalność – właściwość zapewniającą, że działania podmiotu/osoby mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi/osobie;
10) zmiana – działanie lub ciąg działań mających na celu uzyskanie innego stanu systemu teleinformatycznego (konfiguracji lub funkcjonalności) niż przed podjęciem działania.

## § 2.

## Zakres przedmiotowy Regulaminu

1. Niniejszy regulamin odnosi się do rozwoju aplikacji w rozumieniu przyjętych w Regulaminie definicji. Z zakresu Regulaminu jest wyłączona infrastruktura teleinformatyczna oraz platformy aplikacyjne należące do systemu teleinformatycznego ARiMR, których zasady eksploatacji, w tym zarządzania zmianami, są przedmiotem Regulaminu Eksploatacji Systemów Teleinformatycznych.
2. Wymagania bezpieczeństwa dla aplikacji odnoszą się także do platform aplikacyjnych, jeśli z charakterystyki rozwiązania wynika możliwość lub konieczność zaadresowania ryzyk bezpieczeństwa informacji także za pomocą mechanizmów konfiguracji platformy aplikacyjnej.

## § 3.

## Odpowiedzialność za bezpieczeństwo informacji w procesach rozwoju aplikacji

1. W obszarze bezpieczeństwa informacji poszczególnym funkcjom przypisuje się następujące zakresy odpowiedzialności:
    1) Właściciel Procesu/Właściciel Zasobu jest odpowiedzialny za wprowadzenie i nadzór nad realizacją wymagań bezpieczeństwa informacji w procesie powierzonych mu zasobów, w tym opiniuje i konsultuje wymagania bezpieczeństwa na każdym etapie rozwoju aplikacji,
    2) wyznaczony na etapie uruchamiania projektu Kierownik Projektu jest odpowiedzialny za nadzór nad wprowadzeniem i przetestowaniem mechanizmów bezpieczeństwa informacji,
    3) ustanowiony w projekcie Kierownik Obszaru Modyfikacji jest odpowiedzialny za zatwierdzanie wymagań bezpieczeństwa sformułowanych w zapotrzebowaniu na modyfikację,
    4) ustanowiony w projekcie Kierownik Obszaru jest odpowiedzialny za bieżącą kontrolę procesu testowania mechanizmów bezpieczeństwa oraz ich zgodności z zatwierdzonymi wymaganiami bezpieczeństwa informacji oraz za potwierdzanie poprawności procesu instalacji oprogramowania i ewentualnej migracji danych,
    5) osoba wyznaczona przez Kierownika Projektu do prowadzenia Biblioteki Projektu jest odpowiedzialna za formalną kontrolę kompletności dokumentacji oraz jej bezpieczeństwo.
2. W uzasadnionych przypadkach struktura organizacyjna zapewniająca rozwój danej aplikacji może się różnić od powyższej pod warunkiem, że zostaną zachowane zasady realizacji zadań i nadzoru nad ich realizacją określone w niniejszym Regulaminie.

## § 4.

## Wprowadzanie wymagań bezpieczeństwa informacji do specyfikacji wymagań dla aplikacji

1. Właściciel Procesu/Właściciel Zasobu ma obowiązek uzgadniania z dyrektorem komórki właściwej ds. bezpieczeństwa, wymagań bezpieczeństwa informacji przy zgłoszeniu wymagania na aplikację lub modyfikację.
2. Właściciel Procesu/Właściciel Zasobu ma obowiązek zamieszczenia w zgłoszeniu wymagania informacji o wpływie każdej zmiany aplikacji na bezpieczeństwo informacji.
3. Właściciel Procesu/Właściciel Zasobu ma obowiązek uzgadniania z dyrektorem komórki właściwej ds. bezpieczeństwa, dokumentacji przetargowej w zakresie wymagań bezpieczeństwa informacji, jeśli planowany przetarg dotyczy aplikacji lub modyfikacji, w której mają być przetwarzane lub są przetwarzane informacje wrażliwe.
4. Właściciel Procesu/Właściciel Zasobu ma obowiązek dokonać analizy wymagań prawnych w zakresie bezpieczeństwa informacji, zobowiązań umownych oraz

istniejących wewnętrznych aktów normatywnych Agencji w celu zapewnienia zgodności aplikacji lub modyfikacji z tymi wymaganiami. Dyrektor komórki właściwej ds. bezpieczeństwa oraz dyrektor komórki właściwej ds. informatyki mają obowiązek zapewnienia wsparcia merytorycznego dla Właściciela Procesu/Właściciela Zasobu.

5. Wymagania bezpieczeństwa informacji dotyczą funkcji, metod i sposobów przetwarzania oraz wewnętrznych przepływów informacji, które zapewnia aplikacja, zarówno przez mechanizmy wbudowane, jak i zewnętrzne mechanizmy konfiguracyjne w zakresie:
    1) zachowania poufności informacji (jeśli ma zastosowanie),
    2) zachowania integralności informacji oraz integralności przetwarzania informacji,
    3) zachowania dostępności informacji, z uwzględnieniem zdefiniowanych rygorów czasowych oraz poziomów żądanych uprawnień dostępu.
6. W uzasadnionych przypadkach, po konsultacji z dyrektorem komórki właściwej ds. bezpieczeństwa oraz, jeśli ma zastosowanie, z podmiotem zewnętrznym, Właściciel Procesu/Właściciel Zasobu może określić dodatkowe wymagania bezpieczeństwa w zakresie:
    1) potwierdzania autentyczności informacji przez uwierzytelnianie użytkowników lub wewnętrznych procesów aplikacji lub modyfikacji,
    2) zapewnienia rozliczalności użytkowników lub wewnętrznych procesów aplikacji lub modyfikacji przez mechanizmy nadawania uprawnień oraz wewnętrzne mechanizmy logowania aplikacji lub modyfikacji,
    3) niezaprzeczalności wykonania lub niewykonania działania przez użytkownika aplikacji lub modyfikacji,
    4) niezawodności działania aplikacji i modyfikacji.
7. Wymagania integralności przetwarzania informacji w szczególności obejmują:
    1) poprawność przetwarzania danych wejściowych,
    2) poprawność i kompletność zdefiniowanych w dokumentacji analitycznej wewnętrznych procesów aplikacji lub modyfikacji, w szczególności obsługi stanów awaryjnych,
    3) integralność komunikatów przekazywanych i przyjmowanych przez aplikację lub modyfikację,
    4) poprawność przetwarzania danych wyjściowych.
8. W przypadku, gdy zmiana aplikacji lub modyfikacji pozostaje w kompetencji komórki właściwej ds. informatyki bez potrzeby uzyskania akceptacji Właściciela Procesu/ Właściciela Zasobu, to dyrektor tej komórki ma obowiązek przeprowadzenia uzgodnień z dyrektorem komórki właściwej ds. bezpieczeństwa w odniesieniu do wymagań bezpieczeństwa, jeśli mają zastosowanie, na zasadach opisanych w niniejszym paragrafie.
9. Właściciel Procesu/Właściciel Zasobu ma obowiązek zamieścić w dokumentacji przetargowej lub zgłoszeniu wymagania na zmianę aplikacji lub modyfikacji wymagania odnośnie do zaprojektowania i wykonania testowania mechanizmów

zapewniania bezpieczeństwa informacji; wszelkie odstępstwa od wymagania w tym punkcie wymagają aprobaty Komitetu. Dyrektor komórki właściwej ds. bezpieczeństwa oraz dyrektor komórki właściwej ds. informatyki mają obowiązek zapewnienia wsparcia merytorycznego dla Właściciela Procesu/ Właściciela Zasobu.

10. W przypadku aplikacji lub modyfikacji krytycznych z punktu widzenia działalności Agencji, lub w przypadku uzasadnionych wątpliwości, co do spełniania wymagań bezpieczeństwa, Właściciel Procesu/Właściciel Zasobu lub dyrektor komórki właściwej ds. bezpieczeństwa może zwrócić się do dyrektora komórki właściwej ds. informatyki o wykonanie w ramach realizacji umowy handlowej niezbędnych kontroli w zakresie bezpieczeństwa informacji.
11. Umowa z podmiotem zewnętrznym, obejmująca prace rozwojowe nad aplikacjami opracowywanymi na potrzeby i użytkowanymi w Agencji zapewnia:
    1) ustalenie kwestii licencji, własności kodu i praw autorskich,
    2) określenie warunków, w których Agencja, jeśli nie jest właścicielem kodu źródłowego, uzyskuje dostęp do tego kodu (zawarcie umowy typu depozytowego (tzw. „code escrow"),
    3) procedury odbiorów i procedury testów z uwzględnieniem testów z zakresu bezpieczeństwa informacji.
12. W przypadku budowy lub modyfikacji aplikacji tworzonych siłami własnymi przez pracowników Agencji, kierujący komórką/jednostką organizacyjną, na rzecz której jest wykonywana, ma obowiązek zagwarantować przeniesienie na Agencję pełnych autorskich praw majątkowych do aplikacji, zgodnie z obowiązującymi przepisami prawa.

## § 5.

## Kontrola zmian w aplikacjach

1. Zarządzanie zmianami polega na koordynacji, ocenie ryzyka, nadawaniu priorytetów, zatwierdzaniu, planowaniu zasobów w związku ze zmianami dokonywanymi w aplikacjach opracowywanych na potrzeby Agencji.
2. Zmianom, w rozumieniu niniejszego Regulaminu, nie podlega oprogramowanie nabywane na ogólnych warunkach licencjonowania (tzw. oprogramowanie ofoliowane).
3. Zmiany w aplikacji muszą być dokumentowane. Za proces zarządzania zmianami aplikacji odpowiedzialny jest dyrektor komórki właściwej ds. informatyki.
4. Każda zmiana w aplikacji musi być poprzedzona udokumentowanym:
    1) opisem zmiany,
    2) opisem przyczyny zmiany (wraz z podaniem aktów prawnych uzasadniających zmianę – jeżeli ma zastosowanie),
    3) opisem rodzaju wymaganych działań,
    4) szacowaniem ryzyka potencjalnego wpływu zmiany,
    5) harmonogramem wprowadzania zmian,
    6) przetestowaniem aplikacji po wprowadzeniu zmiany.

5. Zmiana, którą trzeba wprowadzić bezzwłocznie, w celu ograniczenia ryzyka poważnego zakłócenia działalności Agencji, wymaga zgody Właściciela Procesu/Właściciela Zasobu i może zostać przeprowadzona z pominięciem zasady określonej w ust. 4 pod warunkiem uzupełnienia dokumentacji towarzyszącej zmianie w najkrótszym możliwym czasie.
6. Zmiany podlegają odnotowaniu w rejestrze zmian prowadzonym przez komórkę właściwą ds. informatyki. Rejestr zmian tworzy zbiór dokumentów opisany w ust. 4.

## § 6.

## Udostępnianie danych przez Agencję w celu wprowadzania zmian w aplikacjach

1. Jeśli prace rozwojowe lub serwisowe związane z aplikacją wiążą się z ujawnieniem informacji wrażliwych, to ich udostępnienie podmiotom zewnętrznym odbywa się wyłącznie pod rygorem uprzedniego zawarcia umowy o zachowaniu poufności, z uwzględnieniem ograniczeń wynikających z Regulaminu ochrony danych osobowych, jeżeli dodatkowo prace wiązać się mogą z dostępem do danych osobowych przetwarzanych przez daną aplikację.
2. Wykorzystywanie do celów testowych szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO, jest zabronione.
3. Wykorzystanie danych rzeczywistych (z wyjątkiem danych wymienionych w ust. 2) jest dopuszczalne tylko w uzasadnionych przypadkach, na podstawie jednorazowego wniosku, lub zatwierdzonego dokumentu projektowego lub umowy powierzenia przetwarzania danych osobowych.
4. Wniosek o zgodę na wykorzystanie danych rzeczywistych w celach testowych, o którym mowa w ust. 3, składa Kierownik Projektu do Właściciela zbioru. Wniosek oraz zgoda Właściciela zbioru dołączana jest do dokumentacji projektowej.
5. W przypadkach szczególnych, gdy prawidłowa weryfikacja zgłoszonego wymagania możliwa jest tylko i wyłącznie w oparciu o dane rzeczywiste, Właściciel zbioru może wyrazić zgodę na wykorzystywanie danych rzeczywistych do celów testowych w ramach wymagania. Zgoda Właściciela odnotowywana jest w dokumentacji projektowej. W przypadku realizowania wymagania przez podmiot zewnętrzny wymagana jest zatwierdzona przez Właściciela zbioru umowa powierzenia przetwarzania danych osobowych uwzględniająca testowanie jako dopuszczoną czynności przetwarzania.
6. Dane rzeczywiste do celów testowych można wykorzystać tylko w odrębnej od eksploatowanej instancji bazy danych. Testowanie na środowisku produkcyjnym jest zabronione.
7. Dostęp do środowiska testowego zawierającego dane rzeczywiste, zarówno logiczny jak i fizyczny, podlega takim samym restrykcjom co dostęp do dla środowiska produkcyjnego.
8. Właściciel zbioru jest informowany o każdorazowym kopiowaniu danych rzeczywistych do środowiska testowego, w przypadkach, o których mowa w ust. 5.
9. Fakt kopiowania danych rzeczywistych do środowiska testowego oraz użycia danych rzeczywistych do celów testowych jest rejestrowany.

10. Po zakończeniu testów dane rzeczywiste muszą być niezwłocznie usunięte ze środowiska testowego.

## § 7.

## Odbiór aplikacji Agencji

1. Kryteria odbioru aplikacji obejmują:
    1) potwierdzenie spełnienia wymagań wydajnościowych i pojemnościowych systemu teleinformatycznego,
    2) potwierdzenie, że instalacja aplikacji nie będzie miała negatywnego wpływu na istniejące systemy, szczególnie w chwilach największego obciążenia (jeżeli ma zastosowanie),
    3) potwierdzenie uwzględnienia wymagań bezpieczeństwa w ramach wykonanej aplikacji,
    4) szkolenia z zakresu funkcjonowania i użytkowania aplikacji,
    5) opracowanie i dostarczenie dokumentacji technicznej, instrukcji dla administratora i użytkownika.
2. Odbioru aplikacji dokonuje Właściciel Procesu/Właściciel Zasobu w porozumieniu z Administratorem Systemu.
3. Oprogramowanie aplikacji jest dostarczane zgodnie z zawartą umową – w postaci kodu wykonywalnego lub źródłowego.
4. Odbiór aplikacji obejmuje następujące główne elementy:
    1) wykonanie instalacji oprogramowania,
    2) dostarczenie przez wykonawcę scenariuszy testów akceptacyjnych,
    3) wykonanie testowania systemu zakończone stosownym dokumentem potwierdzającym prawidłowość testów,
    4) odbiór oprogramowania potwierdzony protokołem,
    5) odrzucenie oprogramowania potwierdzone protokołem, w przypadku negatywnych wyników testów.
5. Każdorazowo, wraz ze zmianą aplikacji, wykonawca dostarcza:
    1) wykaz dokonanych zmian w systemie w stosunku do poprzedniej wersji wraz z ich opisem,
    2) uaktualnienie dokumentacji uwzględniające zmiany dokonane w oprogramowaniu (ujednoliconą dokumentację aplikacji).
6. Po odbiorze nowej aplikacji Właściciel Procesu/Właściciel Zasobu obowiązany jest do zgłoszenia jej do ujęcia w zarządzeniu Prezesa ARiMR w sprawie określenia Właścicieli Zasobów teleinformatycznych. Zmiany zarządzenia dokonuje się zgodnie z zarządzeniem Prezesa ARiMR w sprawie wewnętrznych aktów normatywnych ARiMR.

## § 8.

## Bezpieczeństwo dokumentacji

1. Odpowiedzialność za aktualność i kompletność dokumentacji aplikacji Agencji spoczywa na komórce właściwej ds. informatyki.
2. Biblioteki dokumentacji aplikacji są prowadzone przez Bibliotekę Projektu w komórce właściwej ds. informatyki.
3. Dokumentacja aplikacji jest udostępniana na zasadzie „wiedzy koniecznej”.
4. Wszelki dostęp do bibliotek dokumentacji i kodów źródłowych musi być rejestrowany.
5. Nośniki z kodami źródłowymi są chronione na zasadach określonych w § 4 Polityki i przechowywane w komórce właściwej ds. informatyki.
6. Właściciel Procesu/Właściciel Zasobu zobowiązany jest do przekazania dyrektorowi komórki właściwej ds. informatyki kompletu informacji odnośnie tworzonych siłami własnymi aplikacji, celem zabezpieczenia odpowiednich warunków eksploatacji i utrzymania systemów.