PW_3.6.5-2/Z9

WYTYCZNE DLA DOSTAWCÓW WYKONUJCYCH PRACE PROGRAMISTYCZNE NA RZECZ NCBR (CENTRUM)

1. O ile nie określono inaczej w umowie, dostawca wykonujący prace programistyczne na rzecz Centrum, przekazuje Centrum wytworzony kod źródłowy.
2. Dostawca wytwarza oprogramowanie zgodnie z wymaganiami funkcjonalnymi i pozafunkcjonalnymi określonymi przez Centrum. W przypadku braku wymagań lub wymagań nieprecyzyjnych dostawca podejmuje działania w celu ich zdefiniowania lub doprecyzowania w ramach uzgodnień z Centrum.
3. Dostawcy udostępnia się obowiązujące w Centrum wytyczne dla oprogramowania, w zakresie, w jakim jest to niezbędne z uwagi na prace realizowane przez dostawcę.
4. Dostawca wytwarza oprogramowanie z wykorzystaniem języków programowania, narzędzi i bibliotek uzgodnionych z Centrum.
5. Dostawca zarządza wytwarzanym kodem źródłowym, w tym w zakresie jego przechowywania i wersjonowania, w sposób uzgodniony w Centrum. W szczególności, na polecenie Centrum, dostawca będzie korzystać z repozytorium kodu udostępnionego przez Centrum.
6. Dostawca stosuje konwencję nazewnictwa klas, metod, zmiennych i innych elementów kodu uzgodnioną z Centrum.
7. Dostawca dokumentuje kod w sposób uzgodniony z Centrum. Dokumentowanie kodu dotyczy zarówno komentowania kodu jak i dokumentowania wytwarzanego produktu.
8. Dostawca dokumentuje realizowane prace w sposób uzgodniony w Centrum. W szczególności, na polecenie Centrum, dostawca będzie korzystać z wykorzystywanych przez Centrum narzędzi służących do dokumentowania prac rozwojowych.
9. Dostawca odpowiada za jakość i bezpieczeństwo wytworzonego przez siebie kodu.
10. Dostawca prowadzący prace programistyczne na rzecz NCBR stosuje dobre praktyki w zakresie tworzenia kodu, w tym:
    1) zapewnienie obsługi wyjątków w przypadku wszelkich operacji mogących skutkować wystąpieniem błędu,
    2) przechowywanie poza kodem źródłowym wszelkich parametrów, które mogą wymagać modyfikacji podczas eksploatacji,
    3) przechowywanie danych uwierzytelniających i kluczy kryptograficznych w postaci niejawnej,
    4) stosowanie mechanizmów kryptograficznych uzgodnionych z Centrum,
    5) właściwego zarządzania pamięcią w celu ochrony przed przepełnieniem,
    6) stosowanie kryptograficzne bezpiecznych generatorów liczb losowych,

7) stosowanie bezpiecznej konwersji typów, w szczególności w celu ochrony przed nieakceptowalną utratą informacji,
8) stosowanie ochrony przed bezpośrednim lub pośrednim ujawnieniem danych, w tym informacji o fakcie istnienia lub nieistnienia danych,
9) stosowanie ochrony przed bezpośrednim lub pośrednim ujawnieniem informacji o operacjach niedostępnych dla użytkownika,
10) unikanie bezpośredniego wywoływania poleceń powłoki systemowej,
11) zapewnienie komunikacji z systemem zarządzania bazą danych z wykorzystaniem zapytań parametryzowanych lub procedur składowanych,
12) zapewnienie walidacji wszelkich danych pochodzących ze źródeł zewnętrznych przed znanymi atakami,
13) zapewnienie ochrony przed atakami CSRF,
14) zapewnienie weryfikacji dostępności wszelkich zasobów przed ich użyciem w oprogramowaniu,
15) zapewnienie autoryzacji wszelkich operacji bezpośrednio przed ich wykonaniem,
16) zapewnienie synchronizacji wątków współzależnych w przypadku programów wielowątkowych,
17) wykluczenie możliwości użycia ukrytych kanałów komunikacyjnych w celu nieuprawnionego przekazywania danych.

11. Dopuszcza się korzystanie z zewnętrznego kodu, tj. kodu, który nie został wytworzony przez dostawcę, w tym zewnętrznych bibliotek, o ile powyższe komponenty:
    1) zostały uznane za bezpieczne,
    2) pochodzą z zaufanych źródeł,
    3) zostały pozyskane z zapewnieniem weryfikacji integralności,
    4) mogą zostać wykorzystane zgodnie z warunkami licencji.
12. Dostawca odpowiada za weryfikację i udokumentowanie braku złośliwego kodu w wytwarzanym oprogramowaniu, w tym wykorzystywanych zewnętrznych bibliotekach.
13. Modyfikacja kodu, który nie został opracowany przez dostawcę jest dopuszczalna wyłącznie za zgodą Centrum. Modyfikowanie kodu skutkujące naruszeniem warunków licencyjnych jest zabronione.
14. Wykorzystanie w oprogramowaniu komponentów, które, podczas działania oprogramowania, nie znajdują się w infrastrukturze informatycznej Centrum, jest możliwe wyłącznie za zgodą Centrum.
15. Dostawca odpowiada za przeprowadzanie testów wytwarzanego kodu i ich dokumentowanie. W szczególności testy obejmować powinny elementy związane ze spełnieniem wymagań funkcjonalnych, bezpieczeństwa, wydajnościowych, jak również możliwości integracji z innymi komponentami, z którymi wytwarzane oprogramowanie współpracuje.