Regulamin bezpiecznego użytkowania Centralnego Systemu Teleinformatycznego (CST2021)

Wersja 1.0

Rozdział 1. Słownik pojęć

Użyte w regulaminie określenia oznaczają:

1) System – aplikacje Centralnego Systemu Teleinformatycznego 2021, objęte niniejszym regulaminem:
    1. SL2021 Projekty, umożliwiająca obsługę umów o dofinansowanie oraz rozliczanie projektów,
    2. SR2021, umożliwiająca raportowanie,
    3. SZT2021, umożliwiająca zarządzanie tożsamością użytkownika oraz wspólne logowanie do aplikacji Systemu,
    4. Administracja (w tym eSzop), umożliwiająca zarządzanie uprawnieniami, słownikami oraz opisami programów,
    5. WOD2021, umożliwiająca przygotowanie i obsługę naborów oraz wniosków o dofinansowanie,
    6. e-Kontrole, umożliwiająca prowadzenie i rejestrowanie wyników kontroli projektów.

2) Administrator Merytoryczny – wyznaczony pracownik Instytucji realizujący zadania określone w Wytycznych,
3) Beneficjent – podmiot, o którym mowa w art. 2 pkt 1 ustawy,
4) Dane osobowe – informacje, o których mowa w art. 4 pkt 1 RODO,
5) Incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania Systemu i zagrażają bezpieczeństwu informacji, w tym danych osobowych przetwarzanych w Systemie,
6) Instytucja – Instytucja Koordynująca o której mowa w art.4. 1 ustawy, Instytucja Zarządzająca, o której mowa w art. 71 rozporządzenia ogólnego lub w art. 46 rozporządzenia Interreg, Instytucja Pośrednicząca, o której mowa w art. 2 pkt 10 ustawy, Instytucja Wdrażająca, o której mowa w art. 2 pkt 11 ustawy, lub Instytucja Audytowa, o której mowa w art. 71 rozporządzenia ogólnego lub w art. 45 rozporządzenia Interreg,
7) Ministerstwo – urząd obsługujący ministra właściwego do spraw rozwoju regionalnego,
8) Podatność – luka (słabość) aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w Systemie,
9) Program - program w rozumieniu art. 2 pkt 20 ustawy,
10) Realizator – podmiot korzystający z Systemu w ramach realizacji projektu,
11) RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L. 2016.119.1),
12) Rozporządzenie Interreg - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1059 z dnia 24 czerwca 2021 r. w sprawie przepisów szczegółowych dotyczących celu „Europejska współpraca terytorialna" (Interreg) wspieranego w ramach Europejskiego Funduszu Rozwoju Regionalnego oraz instrumentów finansowania zewnętrznego (Dz. Urz. UE L 231 z 30 czerwca 2021 r.),
13) Rozporządzenie ogólne - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej (Dz. Urz. UE L 231 z dn. 30 czerwca 2021 r.),
14) Ustawa – ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027 (Dz. U. z 2022 r. poz. 1079),
15) Użytkownik - osoba mająca dostęp do Systemu, wyznaczona przez Instytucję do wykonywania w jej imieniu czynności związanych z realizacją programu lub przez Wnioskodawcę, Beneficjenta lub Realizatora do wykonywania w jego imieniu czynności związanych z realizacją projektu,
16) Właściwa instytucja – instytucja odpowiadająca za kontakt z Beneficjentem w sprawach projektu na danym etapie realizacji projektu. Przed podpisaniem umowy jest to instytucja organizująca nabór wniosków o dofinansowanie. Po podpisaniu umowy jest to instytucja, z którą Beneficjent zawarł umowę lub instytucja rozliczająca projekt (jeśli jest inna niż ta, która zawarła umowę),
17) Wnioskodawca – podmiot który przygotowuje lub złożył wniosek o dofinansowanie realizacji projektu, ale nie podpisał jeszcze umowy o dofinansowanie,
18) Wytyczne – Wytyczne ministra właściwego do spraw rozwoju regionalnego w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2021-2027.
19) Zdarzenie związane z bezpieczeństwem informacji – stan Systemu, usługi lub sieci, wskazujący na możliwe naruszenie Regulaminu, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

Rozdział 2. Postanowienia ogólne

1) CST2021 jest systemem centralnym powstałym w oparciu o zapisy ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027, którego wykorzystanie pozwala na wykonywanie:
    a. funkcji Instytucji Zarządzających, o których mowa w rozporządzeniu ogólnym, w szczególności, w zakresie rejestrowania i przechowywania w formie elektronicznej danych dotyczących każdej operacji, niezbędnych do monitorowania, ewaluacji, zarządzania finansowego, weryfikacji i audytów, zgodnie z załącznikiem XVII do rozporządzenia ogólnego,
    b. obowiązku Państwa Członkowskiego polegającego na zapewnieniu odpowiedniej jakości, dokładności i wiarygodności systemu monitorowania i danych dotyczących wskaźników,
    c. obowiązku Państwa Członkowskiego polegającego na zapewnieniu, aby wszelka wymiana informacji między beneficjentami a instytucjami programu odbywała się za pomocą systemów elektronicznej wymiany danych, zgodnie z załącznikiem XIV do rozporządzenia ogólnego.
2) Regulamin wskazuje prawa i obowiązki Użytkowników w obszarach:
    a) korzystania z Systemu,
    b) konfiguracji sprzętu komputerowego Użytkownika,
    c) rozpoczynania, zawieszania i kończenia pracy Użytkowników w Systemie,
    d) korzystania z poczty elektronicznej i Internetu,
    e) zgłaszania usterek, awarii, uszkodzeń oraz podatności i incydentów w Systemie,
    f) przetwarzania danych osobowych w Systemie.
3) Użytkownik, który wprowadza dane do Systemu, jest zobowiązany do zapewnienia ich jakości, w szczególności prawdziwości oraz zgodności ze strukturą danych oczekiwaną przez System.

Rozdział 3. Warunki korzystania z Systemu

1. W celu prawidłowego korzystania z Systemu niezbędne są:
    a) połączenie z siecią Internet;
    b) zainstalowana jedna z wymienionych przeglądarek internetowych we wskazanej wersji major lub nowszej: Mozilla Firefox (wersja 80), Google Chrome (wersja 85), Microsoft Edge (wersja 86) lub Safari (wersja 12),
    c) włączenie obsługi technologii Java Script, akceptacja tzw. "cookies" oraz wyłączenie blokowania wyskakujących okien w przeglądarce internetowej.

2. Ministerstwo nie ponosi odpowiedzialności za brak dostępu do Systemu z przyczyn niezależnych od Ministerstwa.

3. Aplikacje Systemu działają w trybie ciągłym przez 24 godziny na dobę - za wyjątkiem okresu przeznaczonego na przerwę konserwacyjną przypadającą w godzinach od 0:30 do 5:00 (7:00 w przypadku aplikacji SR2021) strefy czasu środkowoeuropejskiego.

4. Ministerstwo, w związku z realizacją prac dotyczących administrowania lub modyfikacji funkcjonalności Systemu, ze względów bezpieczeństwa lub innych przyczyn niezależnych od Ministerstwa, ma prawo czasowo zawiesić dostęp Użytkowników do Systemu w innych godzinach niż podane w ust. 1 na okres niezbędny do wykonania planowanych prac lub wyeliminowania niepożądanych zdarzeń. O planowanych przerwach związanych z prowadzeniem prac konserwacyjnych w Systemie Ministerstwo informuje z wyprzedzeniem.

5. Zabrania się Użytkownikowi nieautoryzowanego monitorowania Systemu w tym jego zabezpieczeń oraz podejmowania wszelkich prób mających na celu naruszenie bezpieczeństwa danych przetwarzanych w Systemie, w tym prób przełamania zabezpieczeń Systemu.

6. System używa plików „cookies” aby ułatwić Użytkownikowi korzystanie z Systemu oraz dla celów technicznych i statystycznych. Jeśli Użytkownik nie zablokuje tych plików, to zgadza się na ich użycie i zapisanie w pamięci swojego komputera lub innego urządzenia. Użytkownik może samodzielnie zmienić ustawienia przeglądarki tak, aby zablokować zapisywanie plików „cookies”, ale uniemożliwi to korzystanie z Systemu.

7. Ministerstwo gromadzi informacje o adresie IP, z którego Użytkownik uwierzytelnia się w Systemie. Ministerstwo gromadzi adresy IP wyłącznie w celu wykrywania prób naruszenia zabezpieczeń Systemu oraz prowadzenia audytu zabezpieczeń Systemu.

8. Ministerstwo nie odpowiada za szkody powstałe w związku z korzystaniem z Systemu, bądź w związku z niewłaściwym działaniem Systemu spowodowanym błędami, brakami, zakłóceniami, defektami, opóźnieniami w transmisji danych, wirusami komputerowymi, awariami łącza sieci Internet lub nieprzestrzeganiem postanowień Regulaminu.

9. Użytkownik jest zobowiązany do zgłaszania przypadków naruszenia bezpieczeństwa informacji lub naruszenia bezpieczeństwa danych osobowych w sposób opisany w Rozdziale 9 tego Regulaminu.

10. Użytkownik może pracować w danej sesji wykorzystując wyłącznie jedno posiadane konto lub kontekst pracy. Zabrania się jednoczesnego uruchamiania kilku sesji przeglądarki/przeglądarek i równoległej pracy w Systemie na więcej niż jednym posiadanym koncie lub kontekście pracy.

11. Ministerstwo zastrzega sobie prawo do zawieszenia konta Użytkownika, który narusza prawo lub postanowienia Regulaminu.

12. Ministerstwo może trwale zablokować konto Użytkownika jeśli Użytkownik nie zaprzestanie działań sprzecznych z prawem lub postanowieniami Regulaminu. Ministerstwo poinformuje właściwy podmiot o zawieszeniu bądź zablokowaniu konta Użytkownika reprezentującego ten podmiot.

Rozdział 4. Dostęp do Systemu

1. Zalogowanie się do Systemu jest możliwe pod warunkiem zarejestrowania konta i ustawienia hasła Użytkownika przez samego Użytkownika lub osobę uprawnioną do zarządzania Użytkownikami w podmiocie, w imieniu którego Użytkownik ma działać w Systemie (administratora). Użytkownik powinien niezwłocznie zmienić hasło nadane przez administratora.

2. Korzystanie z funkcjonalności Systemu jest możliwe pod warunkiem nadania Użytkownikowi uprawnień przez osobę uprawnioną do zarządzania Użytkownikami w podmiocie, w imieniu którego Użytkownik ma działać w Systemie.

3. Uwierzytelnienie Użytkownika następuje w aplikacji SZT przy wykorzystaniu loginu i hasła. Zależnie od przyznanych uprawnień, uwierzytelniony Użytkownik ma następnie dostęp do poszczególnych aplikacji Systemu oraz ich funkcjonalności.

4. Akceptując ten regulamin, Użytkownik zgadza się na otrzymywanie drogą elektroniczną informacji dotyczących Systemu.

5. Ministerstwo udostępnia instrukcje obsługi Systemu na stronie internetowej pod adresem https://instrukcje.cst2021.gov.pl/.

6. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przez siebie w Systemie pracując na własnym koncie przy użyciu loginu i hasła, którymi się posługuje.

Rozdział 5. Zasady bezpieczeństwa

1. Użytkownik jest zobowiązany do zapoznania się i zaakceptowania Regulaminu, co potwierdza (przez złożenie oświadczenia na formularzu elektronicznym) podczas pierwszego logowania w Systemie oraz po zmianie Regulaminu.

2. Złożenie oświadczenia, o którym mowa w pkt. 1, jest warunkiem uzyskania dostępu do Systemu. Informacja o dacie i godzinie złożenia przez Użytkownika oświadczenia jest przechowywana w Systemie.

3. Użytkownik jest zobowiązany do przestrzegania Regulaminu.

4. System jest skonfigurowany zgodnie z następującymi zasadami złożoności haseł:
   a) hasło składa się z minimum 10 znaków (maksymalny rozmiar hasła wynosi 32 znaki),
   b) hasło zawiera wielkie i małe litery oraz cyfry i znaki specjalne,
   c) hasło nie może zawierać w sobie loginu użytkownika,
   d) nowe hasło musi różnić się od wszystkich haseł archiwalnych.

5. Czas trwania nieaktywnej sesji (czas bezczynności), po jakim następuje automatyczne wylogowanie Użytkownika, wynosi 30 minut.

6. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie dokonać zmiany hasła na nowe.

7. W przypadku braku możliwości dokonania przez Użytkownika zmiany hasła (braku działania odpowiedniej funkcjonalności Systemu), należy powiadomić osobę zarządzającą użytkownikami w podmiocie, w którego imieniu Użytkownik działa w Systemie.

8. W celu zapobieżenia nieautoryzowanemu dostępowi do Systemu Użytkownik:
   1) nie może przechowywać danych służących do logowania do Systemu w miejscach dostępnych dla innych osób;
   2) nie może ujawniać danych służących do logowania innym osobom.

9. Zabronione jest korzystanie z Systemu z użyciem danych dostępowych innego Użytkownika.

10. Użytkownik jest zobowiązany do ustawienia ekranu monitora w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.

11. Komputer Użytkownika powinien zostać ustawiony w taki sposób, aby osoby postronne miały utrudniony dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną Użytkownika.

12. Użytkownik jest zobowiązany do przestrzegania zasady czystego biurka. W szczególności przed opuszczeniem stanowiska pracy Użytkownik powinien schować wszelkie dokumenty związane z używanym Systemem oraz informatyczne nośniki danych (dyskietki, płyty CD, DVD, BD, pendrive itp.).

Rozdział 6. Konfiguracja sprzętu Użytkownika

1) Komputer Użytkownika powinien posiadać oprogramowanie antywirusowe, którego sygnatury wirusów powinny być aktualizowane nie rzadziej niż raz na tydzień. Oprogramowanie antywirusowe powinno być stale aktywne.

2) Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej i reagowania na nie.

3) Komputer Użytkownika powinien być chroniony zaporą sieciową (firewall).

4) Podczas pracy z Systemem na komputerze Użytkownika nie powinien być uruchomiony żaden serwer, w szczególności nie powinien być uruchomiony serwer WWW oraz FTP (TFTP).

5) Sprzęt i oprogramowanie powinny być regularnie aktualizowane zgodnie z wytycznymi producentów. W szczególności dotyczy to systemu operacyjnego oraz przeglądarki internetowej.

6) Przeglądarkę internetową należy skonfigurować, aby miała włączoną obsługę protokołu OCSP (Online Certificate Status Protocol), umożliwiającego przeprowadzenie weryfikacji ważności certyfikatu Systemu.

7) Rekomenduje się, aby podczas pracy w Systemie użytkownik nie korzystał z nieznanych lub niezabezpieczonych sieci WiFi.

Rozdział 7. Rozpoczynanie, zawieszanie i kończenie pracy Użytkowników w Systemie

1) Użytkownik podczas logowania się do Systemu jest zobowiązany sprawdzić:
   a. czy w pasku adresowym przeglądarki adres zaczyna się od https,
   b. czy w obrębie okna przeglądarki znajduje się mała kłódka informująca o bezpieczeństwie,
   c. czy po kliknięciu na kłódkę pojawia się informacja o tym, że certyfikat został wydany dla: *.cst2021.gov.pl i jest on ważny.

2) Połączenie do Systemu jest szyfrowane.

3) W celu chwilowego zawieszenia pracy w Systemie, należy zablokować ekran, tj. zablokować pulpit lub włączyć wygaszacz ekranu zabezpieczony hasłem. Jeśli komputer Użytkownika nie pozwala na zabezpieczenie ekranu hasłem, należy wylogować się z Systemu.

4) Po zakończeniu pracy należy wylogować się z Systemu poprzez wybranie funkcji "Wyloguj" zlokalizowanej nad menu w prawym górnym rogu ekranu. Nie należy kończyć pracy poprzez samo tylko zamknięcie okna przeglądarki znakiem „X”.

Rozdział 8. Poczta elektroniczna, Internet

1) W Systemie wykorzystano funkcjonalność wysyłania powiadomień na adres e-mail podany w Systemie. Użytkownik jest zobowiązany do dbania o bezpieczeństwo konta e-mailowego, o którym mowa powyżej, w szczególności poprzez:
   a) używanie silnego hasła dostępu,
   b) nieotwieranie załączników do poczty i linków pochodzących z nieznanych źródeł,
   c) zachowanie ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.

2) Użytkownik powinien korzystać z sieci Internet w sposób, który nie zagraża bezpieczeństwu Systemu.

Rozdział 9. Zgłaszanie zagrożeń bezpieczeństwa

1) W przypadku:
   a) zauważenia podatności,
   b) zdarzenia związanego z bezpieczeństwem informacji,
   c) incydentu,
   d) zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w systemie, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych przetwarzanych w Systemie,

   użytkownik reprezentujący Wnioskodawcę, Beneficjenta lub Realizatora jest zobowiązany do niezwłocznego powiadomienia właściwej Instytucji.

2) W przypadku:
   a) zauważenia podatności,
   b) zdarzenia związanego z bezpieczeństwem informacji,
   c) incydentu,
   d) podejrzenia wystąpienia podatności lub incydentu,
   e) zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w systemie, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych przetwarzanych w Systemie,

   użytkownik reprezentujący Instytucję jest zobowiązany do niezwłocznego powiadomienia Administratora Merytorycznego w tej Instytucji.

3) Użytkownik będący Administratorem Merytorycznym postępuje zgodnie z Procedurą obsługi zgłoszeń w Service Desk Centralnego Systemu Teleinformatycznego.

Rozdział 10. Informacje dotyczące przetwarzania danych osobowych Użytkowników oraz innych danych osobowych wprowadzanych do systemu

1) Administratorami danych osobowych w rozumieniu przepisów RODO są podmioty wskazane w art. 87 ust. 1 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027.
2) Administratorzy przetwarzają dane osobowe w celach określonych w art. 4 rozporządzenia ogólnego.
3) Dane osobowe są przechowywane przez okres niezbędny do realizacji ww. celów, tj. do czasu rozliczenia programów na lata 2021-2027 oraz upływu okresów trwałości i zakończenia kontroli trwałości dla wszystkich projektów.
4) Użytkownik ma obowiązek zachować w tajemnicy przetwarzane dane osobowe oraz informacje o sposobach ich zabezpieczenia, zarówno w okresie korzystania z Systemu jak i po jego zakończeniu.
5) Użytkownik odpowiada za zgodność danych osobowych wprowadzonych przez siebie do Systemu z dokumentami źródłowymi.
6) Każdy Użytkownik ma prawo dostępu do treści swoich danych i ich uzupełnienia, uaktualnienia lub sprostowania.
7) Dane osobowe Użytkowników są przetwarzane w sposób widoczny w Systemie, tj. podczas zarządzania uprawnieniami, odkładania danych audytowych dotyczących wykonywanych czynności oraz podpisywania dokumentów. Użytkownik nie otrzymuje dodatkowej klauzuli informacyjnej na ten temat, innej niż niniejszy regulamin.
8) Każdy Użytkownik ma prawo do wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.