Regulamin Polskiej Federacji Zarządzania Tożsamością ***PIONIER.Id*** na potrzeby realizacji usługi SAML WebSSO

1. Pojęcia wstępne
   1.1. Federacyjne Zarządzanie Tożsamością jest procesem, w którym dostawca usługi świadczonej drogą elektroniczną (zwany dalej ***Dostawcą Usługi***) ufa innemu podmiotowi (zwanemu ***Dostawcą Tożsamości)*** w zakresie zweryfikowania tożsamości i uprawnień użytkownika końcowego. ***Dostawca Tożsamości*** ufa ***Dostawcy Usługi*** w zakresie procedur przetwarzania danych osobowych niezbędnych do świadczenia usługi, które to dane są dostarczane przez ***Dostawcę tożsamości*** w procesie uwierzytelnia i autoryzacji użytkownika.
   1.2. Zaufanie między ***Dostawcą Tożsamości*** a ***Dostawcą Usług***i jest oparte o dwustronne umowy lub inne procedury i ustalenia zastępujące takie umowy.
   1.3. Proces uwierzytelnienia jest chroniony za pomocą parametrów zawartych w opisach technicznych ***Dostawcy Usługi*** i ***Dostawcy Tożsamości*** (tzw. ***metadanych***).
   1.4. Celem tworzenia Federacji Zarządzania Tożsamością jest uproszczenie i zunifikowanie procedur tworzenia umów dwustronnych oraz dostarczenie bezpiecznego źródła metadanych.
   1.5. Federacje Zarządzania Tożsamością mogą zawierać porozumienia o współpracy z innymi Federacjami tworząc konfederacje.

2. Zakres Regulaminu
   2.1. Niniejszy Regulamin określa zasady współdziałania podmiotów w ramach Federacji Zarządzania Tożsamością o nazwie ***PIONIER.Id*** (zwanej dalej także „Federacją PIONIER.Id." albo „Federacją") oraz zasady prowadzenia usług wspomagających procesy federacyjnego zarządzania tożsamością w ramach ***PIONIER.Id***.
   2.2. Polska Federacja Zarządzania Tożsamością ***PIONIER.Id*** stowarzysza podmioty zainteresowane korzystaniem z mechanizmów federacyjnego zarządzania tożsamością.
   2.3. Zespół usług związanych z działaniem federacji ***PIONIER.Id*** będzie nazywany łącznie ***Usługą Federacji PIONIER.Id.***
   2.4. ***Usługa Federacji PIONIER.Id***, której dotyczy niniejszy Regulamin jest świadczona w szkielecie sieci PIONIER przez operatora sieci PIONIER oraz w sieciach członków Konsorcjum PIONIER przez operatorów tych sieci.
   2.5. ***Usługa Federacji PIONIER.Id*** polega na dostarczaniu procedur i środków technicznych niezbędnych do zapewnienia sprawnej współpracy członków i partnerów federacji ***PIONIER.Id*** w celu ułatwienia członkom federacji uwierzytelnionego i autoryzowanego dostępu do usług. ***Usługa Federacji PIONIER.Id*** jest kierowana w pierwszej kolejności do podmiotów należących do sektora badań i edukacji.
   2.6. ***Członkami*** federacji ***PIONIER.Id***, pod warunkiem spełnienia wymagań opisanych poniżej, są usługobiorcy ***Usługi Federacji PIONIER.Id***.
   2.7. ***Partnerami*** federacji ***PIONIER.Id***, pod warunkiem spełnienia wymagań opisanych poniżej, mogą być podmioty świadczące na rzecz usługobiorców Federacji usługi wymagające uwierzytelnionego i autoryzowanego dostępu.
   2.8. Spełnianie wymogów, jakie nakłada członkostwo i partnerstwo federacji ***PIONIER.Id*** gwarantuje, że wszyscy członkowie i partnerzy stosują ten sam minimalny zestaw procedur i pozwala na unifikację zawieranych umów dwustronnych.

3. Organizacja federacji ***PIONIER.Id***
   3.1. Federacja PIONIER.Id w Polsce jest realizowana w oparciu o:
      3.1.1. Regulamin Federacji PIONIER.Id;
      3.1.2. Deklaracje członkowskie Federacji PIONIER.Id;
      3.1.3. Deklaracje partnerskie Federacji PIONIER.Id;
      3.1.4. Umowy w sprawie pełnienia roli Regionalnego Operatora Federacji PIONIER.Id.

3.2. Tryb świadczenia usługi

3.2.1. Usługa Federacji PIONIER.Id może być świadczona albo przez Regionalnego Operatora Federacji albo bezpośrednio przez Operator Federacji;

3.2.2. Operator Federacji może bezpośrednio świadczyć usługę abonentom sieci członków konsorcjum PIONIER do czasu, gdy właściwa dla danej sieci jednostka wiodąca podejmie rolę Regionalnego Operatora Federacji.

3.3. Operator PIONIER.Id

3.3.1. Operatorem Polskiej Federacji Zarządzania Tożsamością PIONIER (PIONIER.Id) w Polsce (National Roaming Operator) jest Instytut Chemii Bioorganicznej Polskiej Akademii Nauk Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS), działające w imieniu Konsorcjum PIONIER.

3.3.2. Zadania Operatora polegają na:

a) koordynowaniu rozwoju Federacji PIONIER.Id w Polsce;
b) nadzorowaniu wdrażania i przestrzegania niniejszego Regulaminu przez członków i partnerów Federacji PIONIER.Id;
c) przyjmowaniu deklaracji w sprawie partnerstwa Federacji;
d) przyjmowanie deklaracji w sprawie członkostwa w Federacji od podmiotów będących bezpośrednimi abonentami sieci PIONIER;
e) przyjmowanie deklaracji w sprawie członkostwa w Federacji od abonentów sieci członków Konsorcjum PIONIER w przypadkach, gdy właściwa dla danej sieci jednostka wiodąca nie podjęła roli Regionalnego Operatora Federacji;
f) koordynowaniu obsługi zdarzeń niepożądanych (nadużyć prawa, etykiety itp.) związanych z działaniem PIONIER.Id;
g) świadczeniu wsparcia służbom technicznym podmiotów będących członkami i partnerami PIONIER.Id, z zastrzeżeniem puntu 3.3.3;
h) prowadzeniu krajowego serwera metadanych Federacji na potrzeby członków i parterów Federacji oraz współpracy międzyfederacyjnej;
i) prowadzeniu serwisu informacyjnego Federacji;
j) udziale w ciałach koordynujących międzynarodowy rozwój technologii i usług Federacyjnego Zarządzania Tożsamością;
k) reprezentowania Federacji PIONIER.Id w działaniach o charakterze międzyfederacyjnym.

3.3.3. Operator ***PIONIER.Id*** nie świadczy wsparcia technicznego użytkownikom końcowym Federacji ***PIONIER.Id***;

3.3.4. Operator ***PIONIER.Id*** nie uczestniczy w procesach przetwarzania danych osobowych związanych z procedurami uwierzytelnienia i autoryzacji i nie bierze żadnej odpowiedzialności za ewentualne naruszenia przepisów o ochronie danych osobowych mogących być wynikiem tych procesów.

3.3.5. Operator ***PIONIER.Id*** może powierzyć część swoich zadań innemu podmiotowi.

3.4. Regionalny Operator ***PIONIER.Id***

3.4.1. Regionalnym Operatorem ***PIONIER.Id*** może być tylko właściwa dla danej sieci jednostka wiodąca MAN lub KDM będąca członkiem Konsorcjum PIONIER.

3.4.2. Przyjęcie roli Regionalnego Operatora PIONIER.Id nie jest obowiązkowe; do czasu podjęcia tej roli przez jednostkę wiodącą, usługa Federacji PIONIER.Id może być świadczona bezpośrednio przez Operatora Federacji.

3.4.3. Zadania Regionalnego Operatora ***PIONIER.Id*** polegają na:

a) reprezentowaniu Federacji wobec swoich abonentów;
b) udzielaniu wsparcia swoim abonentom, korzystającym lub pragnącym korzystać z ***Usługi Federacji PIONIER.Id***;
c) prowadzeniu rejestru swoich abonentów będących członkami ***PIONIER.Id***;
d) przyjmowaniu deklaracji w sprawie członkostwa Federacji ***PIONIER.Id*** od abonentów sieci danego członka Konsorcjum PIONIER, jeżeli podjął się on roli Regionalnego Operatora Federacji;

e) współpracy z krajowym Operatorem ***PIONIER.Id***;

3.4.4. Regionalny Operator PIONIER.ID nie świadczy wsparcia technicznego użytkownikom końcowym.

3.4.5. Regionalny Operator PIONIER.Id nie uczestniczy w procesach przetwarzania danych osobowych związanych z procedurami uwierzytelnienia i autoryzacji i nie bierze żadnej odpowiedzialności za ewentualne naruszenia przepisów o ochronie danych osobowych mogących być wynikiem tych procesów.

3.5. Członkowie federacji PIONIER.Id

3.5.1. Uprawniony podmiot staje się Członkiem Federacji PIONIER.Id w wyniku:

a) zaakceptowania Regulaminu federacji **PIONIER.Id;**

b) podpisania z deklaracji członkowskiej Federacji PIONIER.Id i złożenie jej na ręce właściwego Operatora;

3.5.2. Z chwilą nabycia członkostwa w Federacji Członek Federacji nabywa uprawnienia do korzystania z Usługi Federacji PIONIER.Id i pełnienia funkcji Dostawcy Tożsamości;

3.5.3. Członek Federacji ***PIONIER.Id*** może zostać ***Dostawcą Tożsamości*** pod warunkiem:

a) posiadania narzędzi informatycznych wspierających Federacyjne Zarządzenie Tożsamością i zgodnych z Warunkami Technicznymi Federacji;

b) uzyskania akceptacji przedstawionego Operatorowi Federacji opisu procedur zarządzania tożsamością stosowanych przez Dostawcę Tożsamości;

c) przyjęcia pełnej odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych w szczególności w procesie udostępniania tych danych konkretnym ***Dostawcom Usług***;

d) obligatoryjnego opublikowania przez ***Dostawcę Tożsamości*** lokalnego regulaminu obowiązujący jego użytkowników końcowych w zakresie dostępu do usług objętych regulaminem federacji ***PIONIER.Id***. Regulamin musi zawierać informacje o działaniach i/lub czynnościach, które są niedozwolone podczas korzystania z usługi. ZALECA SIĘ, aby członkowie Federacji uzyskiwali od swoich użytkowników końcowych zaakceptowania potwierdzenia lokalnego regulaminu dostępu do usługi;

e) *obligatoryjnego* prowadzenia przez ***Dostawcę Tożsamości*** wsparcia technicznego dla swoich Użytkowników Końcowych. Członkostwo w ***PIONIER.Id*** nie definiuje konkretnego poziomu jakości (SLA) dla tej usługi, ale zalecane jest, aby członkowie utrzymywali zespoły udzielające wsparcia technicznego swoim użytkownikom w trakcie standardowych godzin pracy w dni robocze;

3.5.4. Członek Federacji MOŻE występować w roli dostawcy usług pod warunkiem spełnienia wymagań dotyczących Partnerów Federacji.

3.6. Partnerzy PIONIER.Id

3.6.1. ***Dostawca Usług*** świadczonych drogą elektroniczną może stać się Partnerem Federacji ***PIONIER.Id*** pod warunkiem:

a) posiadania narzędzi informatycznych wspierających Federacyjne Zarządzenie Tożsamością i zgodnych z Warunkami Technicznymi Federacji;

b) uzyskania akceptacji przedstawianego Operatorowi Federacji opisu procedur zarządzania tożsamością;

c) zaakceptowania Regulaminu Federacji;

d) podpisania deklaracji członkowskiej Federacji PIONIER.Id i złożenie jej na ręce Operatora Federacji;

3.6.2. ***Partner PIONIER.Id*** ponosi pełną odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych w zakresie przetwarzania danych pozyskiwanych od ***Dostawców Tożsamości.***

3.6.3. ***Partner PIONIER.Id*** nie może zgłaszać roszczeń względem ***Operatora PIONIER.Id*** ani ***Operatorów Regionalnych PIONIER.Id*** z tytułu nieprzestrzegania procesów uwierzytelnienia przez ***Dostawców Tożsamości*** i roszczeń takich się zrzeka; z takimi

roszczeniami Partner ***PIONIER.Id*** może występować tylko wobec ***Dostawców Tożsamości***.

3.6.4. ***Partner PIONIER.Id*** musi opublikować politykę przetwarzania i ochrony danych osobowych pozyskiwanych w procesach uwierzytelniania i autoryzacji federacyjnego zarządzania tożsamością.

3.7. Użytkownicy końcowi

3.7.1. ***Użytkownikami końcowymi*** Usługi Federacji PIONIER.Id są osoby fizyczne, których tożsamością elektroniczna zarządzają Dostawcy Tożsamości;

3.7.2. Każdy ***Użytkownik końcowy*** musi być identyfikowany przez co najmniej jednego członka ***PIONIER.Id*** (***Dostawcę Tożsamości***);

3.7.3. ***Użytkownik końcowy*** musi być świadomy, że korzysta z usług oferowanych przez ***Dostawców Usług*** na zasadach publikowanych w lokalnym regulaminie ***Dostawcy Tożsamości***.

4. Wystąpienie z Federacji ***PIONIER.Id***

4.1. Każdy z Podmiotów będących członkiem ***PIONIER.Id***, może w każdym czasie wystąpić z Federacji poprzez zgłoszenie tego faktu na piśmie właściwemu Operatorowi PIONIER.Id. Rezygnacja z członkostwa w PIONIER.Id oznacza automatyczne i natychmiastowe pozbawienie statusu członka PIONIER.Id, zaprzestanie świadczenia Usługi Federacji oraz skasowanie metadanych w zbiorze dystrybuowanym przez serwer Federacji.

4.2. Każdy z Podmiotów będących partnerem ***PIONIER.Id***, może w każdym czasie zrezygnować z partnerstwa poprzez zgłoszenie tego faktu na piśmie Operatorowi PIONIER.Id. Rezygnacja z partnerstwa PIONIER.Id oznacza automatyczne i natychmiastowe pozbawienie statusu partnera PIONIER.Id oraz skasowanie metadanych w zbiorze dystrybuowanym przez serwer Federacji.

5. Odwołanie/zawieszenie Członkostwa

5.1. Prawa członka Federacji ***PIONIER.Id*** mogą być zawieszone lub odebrane w przypadku naruszenia przez Członka regulaminu ***PIONIER.Id***.

5.2. W przypadku wykrycia naruszenia regulaminu przez Członka Federacji, Operator Federacji może dokonać oficjalnego zgłoszenia z podaniem terminu, do kiedy Członek musi przywrócić poprawne i pełne stosowanie regulaminu. Jeżeli po upłynięciu podanego przez Operatora Federacji terminu naruszenie regulaminu nie zostało usunięte, Operator Federacji przekazuje sprawę do, właściwego dla danego Członka, Operatora, który może wydać decyzję o odwołaniu jednostki z członkostwa Federacji i zaprzestaniu świadczenia ***Usługi Federacji PIONIER.Id***.

5.3. Zawieszenie lub pozbawienie członkostwa w PIONIER.Id oznacza automatyczne i natychmiastowe pozbawienie możliwości używania identyfikatorów wystawionych przez tą Jednostkę we wszystkich usługach objętych Federacją PIONIER.Id.

6. Kontrola

Operator jest uprawniony do przeprowadzania weryfikacji przestrzegania zasad niniejszego Regulaminu przez członków i partnerów Federacji PIONIER.Id.

7. Opłaty

7.1. Opłata za korzystanie z Usługi Federacji PIONER Id jest zawarta w opłacie za korzystanie z dostępu do sieci PIONIER lub jednej z sieci członków Konsorcjum PIONIER; jeżeli członek Federacji nie korzysta z takiego dostępu, opłata za korzystanie z usługi PIONIER.Id zostanie ustalona indywidualnie w odniesieniu do każdego przypadku przez Operatora PIONIER.Id;

7.2. Partnerstwo Federacji PIONIER.Id nie pociąga za sobą żadnych zobowiązań finansowych.

8. Odpowiedzialność

8.1. Operatorzy nie są odpowiedzialni za ewentualne szkody wyrządzone przez poszczególnych członków Federacji lub też użytkowników końcowych. Poszczególni Operatorzy nie ponoszą

żadnej odpowiedzialności za brak dostępności do usługi autoryzacji realizowanej bezpośrednio między ***Dostawcą Usługi*** i ***Dostawcą Tożsamości*** lub jej nieprawidłową pracę.

8.2. Członkowie i Partnerzy Federacji zobowiązani są do zapewnienia zgodności z polskimi przepisami, w szczególności z przepisami o ochronie danych osobowych. Operatorzy nie ponoszą żadnej odpowiedzialności za szkody spowodowane nie przestrzeganiem obowiązujących przepisów przez członków i Partnerów Federacji lub użytkowników końcowych.

8.3. Operator federacji PIONIER.Id dołoży wszelkich starań by zapewnić poprawną nieprzerwaną pracę usług Federacji, ale nie ponosi odpowiedzialności finansowej za przerwy lub niewłaściwa pracę tych usług.

8.4. Członkowie federacji ***PIONIER.Id*** są zobowiązani do poinformowania swoich użytkowników końcowych o istnieniu lokalnych zasad użytkowania, które mogą mieć zastosowanie w odniesieniu do usług świadczonych za pośrednictwem mechanizmów Federacji PIONIER.Id.