This document contains a “best effort” translation of its Polish original. It is provided for information only. The only legally binding document is the original in Polish.

Polish Identity Federation PIONIER.Id
SAML WebSSO Policy

1. Introduction
   1.1. Federated Identity Management is a process in which a provider of an information service (further called the **Service Provider**) trusts another entity (called the **Identity Provider**) with end user identity verification and authorization. The Identity Provider trusts the Service Provider’s operational procedures with respect to the handling of personal data required by the service and supplied by the Identity Provider in the process of user authentication and authorization.
   1.2. The trust between the Service Provider and the Identity Provider is based on bilateral agreements or other procedures replacing such agreements.
   1.3. The authentication process is protected by the technical parameters contained in the Service Provider and Identity Provider metadata
   1.4. The reason for creation of an Identity Federation is to simplify and unify the procedures of setting up of bilateral agreements and provide a safe metadata source.
   1.5. Identity Federations may enter into cooperation agreements by creating confederations.
2. Scope
   2.1. This Policy defines the rules of interaction between entities within the Identity Federation named ***PIONIER.Id*** (further called ***PIONIER.Id Federation*** or simply ***Federation***) and the rules of running services supplementing the processes of federated identity management in ***PIONIER.Id***.
   2.2. The ***Polish Identity Federation PIONIER.Id*** federates entities interested in using the federated identity management.
   2.3. The set of services resulting from the activities of the ***PIONIER.Id Federation*** will be called jointly the ***PIONIER.Id Federation Service***.
   2.4. The ***PIONIER.Id Federation Service*** covered by this ***Policy*** is provided in the core PIONIER network by the PIONIER network operator and in the networks of PIONIER Consortium members by the operators of these networks.
   2.5. The ***PIONIER.Id Federation Service*** supplies procedures and technical means required for efficient cooperation between the Federation members and partners in order to simplify authenticated and authorized access to services. The ***PIONIER.Id Federation Service*** is primarily addressed to the members of R&D and Higher Education community.
   2.6. ***PIONIER.Id Federation Members*** are, under the terms described below, the consumers of the ***PIONIER.Id Federation Service***.
   2.7. ***PIONIER.Id Federation Partners*** can be, under the terms described below, any entities providing such services for Federation members which require authenticated and authorised access.
   2.8. Adherence to the requirements set by the ***PIONIER.Id*** membership and/or partnership guarantees that all members and partners use the same minimal set of procedures and thus simplifies the unification of bilateral agreements.
3. Organisation of the ***PIONIER.Id Federation***
   3.1. ***PIONIER.Id Federation*** is based upon:
      3.1.1. PIONIER.Id Federation Policy;
      3.1.2. PIONIER.Id Federation Membership declarations;
      3.1.3. PIONIER.Id Federation Partner declarations;
      3.1.4. Regional Federation Operator agreements.

3.2. Service provisioning

3.2.1. The ***PIONIER.Id Federation Service*** can be provided either by the Regional Federation Operator or directly by the Federation Operator;

3.2.2. Federation Operator can provide the service directly to the clients of a PIONIER Consortium member network until the proper network operator decides to take the role of the Regional Federation Operator.

3.3. PIONIER.Id Federation Operator

3.3.1. The role of the Federation Operator in Poland is performed by the Institute of Bioorganic Chemistry of the Polish Academy of Sciences – Poznan Supercomputing and Networking Center (PSNC), acting on behalf of the PIONIER Consortium.

3.3.2. Operator's duties:

a) coordination of the Federation growth;
b) monitoring the acceptance and adherence to the Federation Policy by members and partners of the Federation;
c) accepting Federation Partner declarations;
d) accepting Membership declarations from entities being direct PIONIER clients;
e) accepting Membership declarations from entities being the clients of a PIONIER Consortium member network in cases where the corresponding Regional Federation Operator has not been established;
f) coordination of incident handling (law or etiquette violation etc.) when they relate to the PIONIER.Id Federation;
g) providing support to technical staff of Federation members and partners, with the exception stated in 3.3.3;
h) providing and administering a national Federation metadata server for the use of members and partners of the Federation and international cooperation;
i) providing and administering Federation information service;
j) participation in international bodies coordinating federated identity management technology and services;
k) representing the PIONIER.Id Federation in interfederation projects.

3.3.3. PIONIER.Id Operator does not provide support for end users of the Federation.

3.3.4. PIONIER.Id Operator does not participate in processing of personal data which might be a part of the authentication and authorization and therefore takes no responsibility for any resulting violation of regulations.

3.3.5. PIONIER.Id Operator can subcontract part of its duties to another entity.

3.4. Regional PIONIER.Id Operator

3.4.1. Only the PIONIER Consortium member can be the Regional Federation Operator for its network.

3.4.2. Acceptance of the role of the Regional Federation Operator is optional; until this happens the PIONIER.Id Federation Service can be provided by the Federation Operator.

3.4.3. Regional Federation Operator's duties:

a) representing the Federation for its network clients;
b) supporting its clients using or planning to use the Federation Service;
c) administering the registry of its clients which are the Federation Members;
d) accepting Federation Membership declarations from its clients;
e) cooperation with the Federation Operator.

3.4.4. Regional Federation Operator does not provide support for end users of the Federation.

3.4.5. Regional Federation Operator does not participate in processing of personal data which might be a part of the authentication and authorization and therefore takes no responsibility for any resulting violation of regulations.

3.5. PIONIER.Id Federation Members

3.5.1. An eligible entity becomes the member of the PIONIER.Id Federation as a result of:
   a) accepting the Federation Policy;
   b) signing the Federation Membership Declaration and delivering it to the proper Operator.

3.5.2. Federation Member has rights to use the Federation Service and play the role of the Identity Provider;

3.5.3. PIONIER.Id Federation Member may become an Identity Provider under the following conditions:
   a) possessing IT tools supporting federated identity management compliant with the Federation Technical Terms;
   b) obtaining an acceptance of the description of its identity management procedures from the Federation Operator;
   c) accepting a full responsibility for following the Personal Data Protection law and in particular for sharing personal data with Service Provides;
   d) publishing a local policy targeted at its end users and describing regulations for accessing services covered by the Federation policy. Such policy must contain information about prohibited actions. It is recommended that Federation Members obtain confirmation from its uses of the local policy.
   e) providing support for its End Users; Federation Membership does not define an SLA for such support, but it is recommended that it is available during standard office hours on working days.

3.5.4. A Federation Member MAY act in the role of a Service Provider, provided it fulfils the terms required for Federation Partners.

3.6. PIONIER.Id Federation Partners

3.6.1. An electronic service provider may become the Federation Partner under the following conditions:
   a) possessing IT tools supporting federated identity management compliant with the Federation Technical Terms;
   b) obtaining an acceptance of the description of its identity management procedures from the Federation Operator;
   c) accepting the Federation Policy;
   d) signing the Federation Partner Declaration and delivering it to the proper Operator.

3.6.2. Federation Partner takes the full responsibility for acting accordingly to Personal Data Protection law with respect to personal data obtained from the Identity Providers.

3.6.3. Federation Partner cannot make any claims against the Federation Operator or Regional Federation Operators under the title of any authentication process breach caused by the Identity Providers and declines the right to such claims; Federation Partner can only make claims towards the Identity Providers.

3.6.4. Federation Partner must publish a privacy policy describing data processing and protection of data obtained during the federated authentication and authorization process.

3.7. End Users

3.7.1. The End Users of the PIONIER.Id Federation service are persons, whose electronic identity is managed by Identity Providers.

3.7.2. Each End User must be identified by at least one PIONIER.Id Member (Identity Provider).

3.7.3. The End User must be aware that he is using services offered by a given Service Provider under the terms published in the local policy of the Identity Provider.

4. Leaving the PIONIER.Id Federation

4.1. Each Member of the PIONIER.Id Federation my leave the Federation at any time by presenting a written resignation to the proper Operator. Leaving the Federation results in

automatic and immediate deprivation of membership status, withholding the Federation Service for the given entity and deletion of the entity metadata from the Federation metadata set.

4.2. Each Partner of the PIONIER.Id Federation my leave the Federation at any time by presenting a written resignation to the Federation Operator. Leaving the Federation results in automatic and immediate deprivation of partner status and deletion of the entity metadata from the Federation metadata set.

5. Revocation/suspension of Membership
   5.1. Membership rights of a Federation Member may be suspended or revoked in the case of Policy violation by the Member.
   5.2. In the case of a Policy violation by a Federation Member, the Federation Operator may send an official notification containing the deadline for rectification of the problem. If, after this deadline, the violation has not been rectified, the Federation Operator passes the case to the proper Operator who may decide to revoke the membership and stop the provisioning of the Federation Service.
6. Inspection
   6.1. The Federation Operator is authorized to verify the observance of this Policy by Members and Partners of the PIONIER.Id Federation.
7. Fees
   7.1. Federation Service fee is contained in the fee for using either the PIONER network or one of the networks of the PIONIER Consortium members; if a Federation Member does not pay such a network access fee, then the fee for using the Federation Service will be set by the Federation Operator individually for each case.
   7.2. Federation Partnership is free of charge.
8. Liability
   8.1. The Operators are not liable for any damages caused by Federation Members or End Users. Individual Operators do not take any responsibility for a lack of authentication service realised directly between an Identity Provider and a Service Provider or incorrect behaviour of such a service.
   8.2. Federation Members and Partners are responsible for compliance with the Polish law, in particular for protection of personal data. The Operators are not liable for any damages caused by a violation of rules and regulations by the Federation Members or Partners and by the End Users.
   8.3. The PIONIER.Id Federation Operator will make every effort to ensure correctness and continuity of the Federation Service, but will not accept any financial liability for errors or discontinuity of the service.
   8.4. Federation Members are responsible for informing their users about the existence of local policies, which could be relevant for services provided with the use of the Federation tools.