Participation agreement for the South African Identity Federation (SAFIRE)

DRAFT!!! version 2016-09-16

Entered into between

Tertiary Education and Research Network of South Africa NPC

A Non-Profit Company incorporated in terms of the Companies Act,
Registration Number: 2000/020780/08

(hereinafter referred to as "TENET" or the "Federation Operator")

and

_____

Name of participating organisation

(hereinafter referred to as the "Participant")

who designates the following contact people for the purposes of §6.2.1 of this agreement:

	Organisational contact	**Technical contact**
Name		
Email address		
Contact number		

1. Preamble

1.1. Introducing SAFIRE

1.1.1. Identity Federations are associations of organisations that come together to exchange information, as appropriate, about their End Users and resources in order to facilitate and enable collaboration and transactions.

1.1.2. The South African Identity Federation (SAFIRE) exists to coordinate and facilitate such federated activities for the research and higher education communities in South Africa. It does so by making use of various federation technologies to extend the scope of digital identities (user credentials) issued by one federation Participating Party to be valid across the whole federation. In some instances, it further facilitates inter-federation with other national federations around the world.

1.1.3. Federations can make use of a number of different technologies to achieve a roughly analogous purpose. Whilst SAFIRE was established with a single technology (SAML2) in mind, it is organisationally structured to be technology agnostic and to allow for various Technology Profiles. A set of technical requirements and practices documents each Technology Profile.

1.1.4. An Identity Provider (IdP) is responsible for authenticating its own end users by checking the credentials against a local identity management system. Identity Providers make assertions about the identity of their End Users, and a subset of these assertions is relayed to Service Providers when required. As they hold information about the organisation an End User is affiliated with, Identity Providers are often referred to as an End User's Home Organisation or Home Institution and the terms are sometimes used interchangeably.

1.1.5. A Service Provider (SP) provides services (such as access to a web site or network) to End Users once they are successfully authenticated. For this reason, Service Providers are often and interchangeably referred to as an end user's Visited Organisation or Visited Institution.

1.1.6. A Federation Operator performs a coordinating role — it provides the necessary metadata and/or infrastructure to ensure that authentication requests from the Service Provider reach the right Identity Provider, which may involve passing such information to other operators in other countries. The Federation Operator also maintains governance and oversight of the federation within the country in which they operate. TENET is the Federation Operator of SAFIRE. Depending on the Technology Profile in use, a Federation Operator may be known interchangeably as the Roaming Operator.

1.2. Federation trust relationships

1.2.1. In order to work successfully, all identity federations depend on an implicit tripartite trust relationship between an Identity Provider, a Service Provider, and one or more Federation Operators.

1.2.2. The Identity Provider advertises services to its End Users, and trusts that the Service Provider will provide the service in a manner consistent with expectations. Identity Providers further trust that Service Providers will secure their users' personal information and respect the confidentiality of their users' communications.

1.2.3. Service Providers trust that the End User identities asserted by an Identity Provider are bona fide members of their organisation in good standing, and that an Identity Provider has a binding agreement with those users in the form of an acceptable use policy or equivalent. Service Providers trust that Identity Providers will take action in terms of their organisational policies should abuse be reported. Some Service Providers have legal or governance obligations to retain information about the people they provide service to, and trust that Identity Providers will do so on their behalf in exchange for reducing the complexity of gaining access.

1.2.4. Both Identity Providers and Service Providers trust Federation Operators to both provide the necessary infrastructure and oversight, to act as a trusted introducer, and to respect the privacy of their respective users and their communications.
1.2.5. One of the founding principles of such a relationship is a clear understanding by all parties of their respective roles and responsibilities.

1.3. Purpose of this agreement

1.3.1. This document is intended to serve as a lightweight participation agreement, whereby the parties formally acknowledge their respective roles in making SAFIRE successful. It is expected that the parties to this agreement enter into a good-faith relationship and thus, where the agreement fails to adequately cover a particular aspect, will work together to achieve constructive resolution.
1.3.2. It is not the sole document governing participation in SAFIRE, but forms the overarching framework under which the associated governance structures, policy, and practice statements exist.

2. Joining & withdrawal

2.1. Eligibility

2.1.1. Any organisation that has signed this participation agreement may participate in SAFIRE.
2.1.2. Any Participant who is able to meet the necessary technical and administrative requirements may become a Service Provider, save that at least one existing Identity Provider must first indicate that they will make use of the Service Provider's services.
2.1.3. Eligibility to become an Identity Provider is limited to a subset of Participants, and that subset may vary according to the Technology Profile in use. Details of the eligibility to participate as an Identity Provider for a given Technology Profile may be published on SAFIRE's web site and is available from TENET.
2.1.4. Identity Providers must operate with institutional-level authority. In general this means that only one Identity Provider per Participant should be admitted.
2.1.5. Only those Identity Providers who are contributing financially to SAFIRE and who are fully-paid up are considered Members of SAFIRE, and are therefore eligible for the benefits of membership.

2.2. Joining

2.2.1. Eligible Participants may join SAFIRE by completing and signing this participation agreement, confirming their canonical or legal name, and by appointing technical and administrative contacts to liaise with SAFIRE.
2.2.2. Participants who wish to act as Identity or Service Providers within a given Technology Profile must further meet the technical requirements for participation in that profile.

2.3. Withdrawal

2.3.1. A Participant may withdraw from SAFIRE by providing one (1) calendar month's written notice.
2.3.2. Those Members who have paid fees in advance shall not be eligible for a refund on withdrawal.
2.3.3. On withdrawal, the Participant must cease using the SAFIRE name, logo or brand in association with any services.

3. Costs

3.1. Service Providers

3.1.1. SAFIRE makes its services available to Service Providers free-of-charge.

3.2. Identity Providers

3.2.1. Identity Providers are expected to contribute financially towards SAFIRE. However the exact cost structures have not been finalised at the time of concluding this agreement.

3.2.2. By signing the participation agreement and acting as an Identity Provider, the Participant acknowledges that they will become liable for fees in future, and that the Federation Operator will invoice them for such on a monthly or annual basis.

3.3. Changes to cost structures

3.3.1. All cost structures are subject to annual escalation to accommodate changes in costs of delivering the service.

3.3.2. The Federation Operator gives an undertaking that no new cost structures will be introduced unless three (3) calendar months' notice has been given, and that existing Participants will be able to withdraw without penalty during that notice period.

3.3.3. For the avoidance of doubt, §3.3.2 includes the cost structures described by §3.2.2.

4. Relationship in terms of the Protection of Personal Information Act, 2013

4.1. SAFIRE may receive personal information about data subjects from an Identity Provider, process such information in terms of its standard operating practices, and subsequently re-release a subset of that personal information to a Service Provider. For this reason it is important to clarify the various parties' roles in terms of the Protection of Personal Information Act, 2013.

4.2. SAFIRE's standard operating practices are formulated in collaboration with participating Identity and Service Providers, and are typically published on its website in the form of various practice statements. They include, but are not limited to, the filtering and transformation of various Attributes forming the personal information of the data subject; the negotiation of Attribute Release Policies; collection of consent from the data subject; publishing of organisational information in metadata; and acting as a proxy for authentication and authorisation requests.

4.3. By participating in SAFIRE, Identity and Service Providers acknowledge SAFIRE's operating practices, and give instruction to SAFIRE to process personal information about data subjects according to those practices.

4.4. Identity Providers are the "responsible party" (or data controller) for personal information about those data subjects for whom they make assertions and SAFIRE (and the underlying Federation Operator) acts as the Identity Provider's "operator" as defined in the Protection of Personal Information Act, 2013 (or more generally, as a data processor as understood by many other jurisdictions).

4.5. This Participation Agreement does not confer any instruction or special rights upon Service Providers. For this reason, SAFIRE will, by default, request the data subject's consent before passing personal information to a Service Provider.

4.6. However, it is acknowledged that individual Identity and Service Providers may enter into separate data processing agreements and that these could facilitate the Service Provider acting as an "operator" (or data processor) on behalf of the Identity Provider. Thus, on written instruction to this effect from an Identity Provider, the requirement for consent may be waived.

4.7. In the special case of inter-federation, Service Providers are the "responsible party", and instruct SAFIRE to act as their "operator" and process personal information received from third-party identity providers who are not direct Participating Parties within the SAFIRE federation.

5. Inter-federation

5.1. In order to facilitate collaboration across national and organizational borders the Federation Operator may participate in inter-federation agreements. How the potential inter-federation agreement operates administratively and technologically depends on the Technology Profile.

5.2. The Participant understands and acknowledges that via those inter-federation arrangements the Participant may interact with organizations which are bound by and committed to foreign laws and federation policies. Those laws and policies may be different from the laws and policies in this Federation.

6. Responsibilities

6.1. Responsibilities of the Federation Operator

6.1.1. The Federation Operator should insofar as is possible act in the best interests of the Participants.

6.1.2. The Federation Operator is responsible for ensuring that the SAFIRE infrastructure meets the requirement of the Technology Profiles, and for meeting the service levels described in section 7 below.

6.1.3. The Federation Operator will provide limited technical support to the Participant's designated contacts in line with the Technology Profiles. However, it is not responsible for the implementation of Identity or Service Providers or for integration with the Participant's identity management systems.

6.1.4. For the purposes of establishing the trust relationship described in section 1.2 above and to facilitate inter-federation as described in section 5, the Federation Operator must produce practice statements that describe its standard operating practices and make these statements publicly accessible on its web site.

6.1.5. Where the Participant is an Identity Provider and has delegated responsibility for negotiating Attribute Release Policies to the Federation Operator, the Federation Operator must act at all times according to the principles of minimality – personal information processed, transmitted or stored must be adequate, relevant and not excessive.

6.1.6. To meet its obligations as an "operator", the Federation Operator must implement reasonable technical and organisational security measures to prevent personal information from being accidentally or illegally lost, destroyed, or made available to unauthorised parties.

6.2. Responsibilities of all Participants

6.2.1. Participants must designate at least one technical and one organisational contact person, and to make sure that SAFIRE is kept appraised of any changes thereof.

6.2.2. Participants must provide SAFIRE with documentary evidence of their canonical or legal organisational name, and keep SAFIRE appraised of changes thereto.

6.2.3. Participants must meet or exceed the Technical Profile(s) for any federation technologies they deploy. This includes maintaining adequate logging (typically retaining logs of successful authentication requests for at least 180 days), and ensuring automated updates of metadata or other Federation information.

6.2.4. Participants should ensure that the (IT) security of the own organisation complies with prevailing good practices – should SAFIRE have reason to believe that a system connected directly or indirectly to the Federation may significantly compromise security, it may disconnect such system until the issue is resolved (see §8).

6.2.5. Participants are expected to act as first-line support for their services or end users. They must publish up-to-date contact details for their help desk (or equivalent support structure) in the

appropriate place depending on Technology Profile. Such a help desk should be available to their end users at least during normal office hours in their home time zone.

6.2.6. Participants must cooperate with the Federation Operator and other Participating Parties in resolving incidents and should report incidents to the Federation Operator in cases where these incidents could negatively affect the security, trustworthiness or reputation of the Federation or any of the Participating Parties.

6.3. Responsibilities of Identity Providers

6.3.1. Identity Providers should produce an Identity Management Practice Statement that describes their identity management lifecycle, including how individual end users are enrolled, maintained and removed from their identity management systems, as well as their level(s) of assurance of individual data subjects.

6.3.2. Identity Providers must provide the minimum set of information or Attributes required for the Technology Profile(s) they deploy. In addition, they are strongly encouraged to provide all recommended Attributes.

6.3.3. Identity Providers must ensure that all and any Attributes they assert are accurate and up-to-date, and that changes thereto are reflected timeously.

6.3.4. Should an end user cease to be affiliated with an Identity Provider, the Identity Provider must cease asserting their identity as soon as practically possible (usually within one working day).

6.3.5. Identity Providers must ensure that any end user whose identity they assert is bound by their organisational acceptable use policies. Such policies must allow for sanction in case of abuse irrespective of an end user's geographic location at the time of the breach. Identity Providers must not assert the identity of any end user who is not bound by such policy.

6.3.6. Identity Providers are responsible for the enforcement of their organisational acceptable use policies, and should take appropriate action where incidents of abuse are reported by visited organisations.

6.4. Responsibilities of Service Providers

6.4.1. Service Providers are responsible for making the decision on which end users can access the services they operate and what access rights they are granted. Additionally, it is the Service Provider's responsibility to implement those decisions.

6.4.2. Service Providers must document how they handle personal information in a privacy statement, and should make that privacy statement available in an appropriate way depending on the Technology Profile.

6.4.3. Service Providers may not provide personal information received via SAFIRE or any inter-federation service to any other party without the **explicit** consent of the data subject, unless otherwise allowed for by contract with the individual Identity Provider concerned or required by South African law.

6.4.4. When requesting Attributes, Service Providers must respect the principle of minimality – personal information processed or stored must be adequate, relevant and not excessive in accordance with the stated purpose of the service.

6.5. Operating on a "best effort" basis

6.5.1. It is acknowledged that SAFIRE is in the early stages of development; that both technology and policy may evolve as the federation matures; and that many organisations that may wish to become Participants may not have sufficient internal operational maturity to implement the technical and administrative controls expected by the federation trust model.

6.5.2. Whilst these impose very real limitations, it is not intended that they become impediments to the early and rapid deployment of identity federation in South Africa.

6.5.3. Thus both the Participant and the Federation Operator must undertake to use all reasonable endeavours to comply with the spirit of this participation agreement and its associated policy and practice statements on a “best effort” basis, and to communicate clearly with each other where shortfalls may occur.

7. Service levels

7.1. The Federation Operator will endeavour to keep all critical components of SAFIRE operational at all times, save for scheduled maintenance.

7.2. However, as noted in §6.5, the Federation operates on a best effort basis and thus the intent signified by §7.1 is limited by what is currently technically and organisationally possible. The Federation Operator undertakes to communicate realistic expectations of availability to all Participating Parties.

7.3. Scheduled maintenance will occur during the Federation Operator’s standard maintenance windows, as published from time to time on the SAFIRE web site.

7.4. Emergency maintenance may be undertaken at any time.

8. Occasion for sanction

8.1. It is intended that any breaches of this participation agreement, or the associated policies, practice statements, or Technical Profiles be resolved by negotiation in good faith.

8.2. Notwithstanding §8.1, a serious breach that may compromise the security or integrity of SAFIRE’s services or the privacy of any data subject constitutes grounds for immediate temporary suspension of SAFIRE services pending the outcome of such negotiations or – should negotiation prove unsuccessful – mediation as described in §11.3 below.

8.3. Likewise, the Federation Operator may take whatever immediate actions are deemed necessary to maintain the operational stability and integrity of SAFIRE services for the majority of Participating Parties, even if that occurs at the expense of an individual Participant.

8.4. Such sanctions as described in this section shall only be imposed for the shortest period necessary.

9. Limitation of liability

9.1. The Federation Operator offers this service on an “as is” basis, without any warranties or liabilities to the Participant or its End Users. Neither SAFIRE, TENET, nor any of its staff, agents, or subcontractors shall be liable for impact or damages caused by failure, downtime, unavailability, or errors of the Federation or any of the Technology Profiles.

9.2. The Participant is required to ensure compliance with applicable laws. Neither SAFIRE, TENET, nor any of its staff, agents, or subcontractors shall be liable for damages caused by failure to comply with any such laws on behalf of the Participant or its End Users relating to the use of the Federation services.

9.3. The Federation makes no warranties about the correctness or fitness-for-purpose of any Attributes or other data it receives from Identity Providers, processes or transforms, and re-releases to Service Providers. The level of assurance of such Attributes should be determined from the individual Identity Providers’ Identity Management Practice Statement.

10. Commencement and changes

10.1. This participation agreement becomes effective once it is signed by both parties.

10.2. Substantive changes to the participation agreement may require the Participant to sign a new agreement. Should this not happen within one (1) calendar month of notification, the Participant will be deemed to have voluntarily withdrawn from the Federation.

10.3. All changes to policy and standard operational practices become effective thirty-two (32) days after their publication on the Federation Operator's web site. If the Participant does not give notice to withdraw before the effective date, they are deemed to have tacitly consented to such changes and issued new processing instructions to the Federation Operator.

11. General provisions

11.1. Irrespective of the domicile of the Participant, this participation agreement is governed by, and construed in accordance with, the laws of the Republic of South Africa and the High Court of South Africa shall have jurisdiction.

11.2. If any provision of this participation agreement is held to be unenforceable by any court of competent jurisdiction, all other provisions will nevertheless continue in full force and effect.

11.3. Processes for handling disputes, mediation, arbitration, and breach shall be as described in the corresponding sections of TENET's prevailing REN Service Agreement, irrespective of whether the Participant is a signatory to that agreement.

11.4. The Federation Operator may elect to outsource the provision and/or operation of some or all of the technical infrastructure to another party of its choosing. Any reference to the Federation Operator in this document must be taken to include both the Federation Operator and/or its appointed agents or subcontractors as appropriate.

Signed for and on behalf of SAFIRE – South African Identity Federation

at _____ on this the _____ day of _____ 20___:

_____ _____

Signatory warrants that they are duly authorised thereto *As witness*

Signed for and on behalf of the Participant

at _____ on this the _____ day of _____ 20___:

_____ _____

Signatory warrants that they are duly authorised thereto *As witness*

Appendix – Definitions

Most of these terms should be contextually defined in the text. However, if we need a clearer set of definitions, we can use these:

Term	Meaning
Attribute	A piece of information describing the End User, his/her properties or roles in an organisation.
Attribute Release Policy	The specific set, negotiated of Attributes that gets released to a Service Providers or a specific set of Service Providers.
Data Subject	As defined in POPI; an End User about whom we have personal information.
End User	Any natural person affiliated to a Home Organisation, e.g. as an employee, researcher or student making use of the service of a Service Provider.
Federation Operator, Roaming Operator	Generically, the organisation providing and operating infrastructure for authentication and authorization to members of or participants in an Identity Federation. In the specific SAFIRE case, the Federation Operator is TENET.
Federation, Identity Federation	An association of organisations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
Identity Provider, Home Organisation	The organisation with which an End User is affiliated. It is responsible for authenticating the End User and managing End Users' digital identity data.
Identity Management Practice Statement	A document that formally an Identity Provider's identity management lifecycle, including how individual end users are enrolled, maintained and removed from their identity management systems, as well as their level(s) of assurance of individual data subjects.
Member	The subset of Participating Parties (and specifically Identity Providers) who contribute financially towards SAFIRE and are therefore eligible for the benefits of membership – such as participating in governance structures.
Participant	Any organisation that has signed this participation agreement and wishes to participate in SAFIRE.
Participating Parties	The collection of organisations participating in SAFIRE, including the Participant.
Service Provider, Visited Organisation	An organisation that is responsible for offering the End User the service they desire to use. Service Providers may rely on the authentication outcome and attributes that Home Organisations assert for its End Users.
Technology Profile	The set of documents that defines how a specific federation technology (e.g. SAML2) is deployed within SAFIRE.