Identity Federation Policy

1 Document Control

ROLE	NAME	TITLE	DATE	SIGNATURE
Prepared by	Zanga Chimombo	Systems Manager	18 Dec 2023	
Approved by	Solomon Dindi	CEO		

2 Revision Control

VERSION	DATE	AUTHOR	DESCRIPTION OF CHANGES
1.0	18 Dec 2023	Zanga Chimombo	First draft.
2.0	03 Dec 2024	Jones Kumwenda	Updated the formatting

Table of Contents

3 Definitions and Terminology

Attribute:	A piece of information describing the End User, his/her properties or roles in an organization.
Attribute Authority:	An organization responsible for managing additional Attributes for an End User of a Home Organization.
Authentication:	Process of proving the identity of a previously registered End User.
Authorization:	Process of granting or denying access rights to a service for an authenticated End User.
Digital Identity:	A set of information that is attributable to an End User. Digital identity consists of Attributes. It is issued and managed by a Home Organization and zero or more Attribute Authorities on the basis of the identification of the End User.
End User:	Any natural person affiliated to a Home Organization, e.g. as an employee, researcher or student making use of the service of a Service Provider.
Federation:	An association of organizations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
Federation Operator:	Organization providing Infrastructure for Authentication and Authorization to Federation Members.
Federation Member:	An organization that has joined the Federation by agreeing to be bound by the Federation Policy in writing. Within the

federation framework, a Federation Member can act as a Home Organization and/or a Service Provider and/or an Attribute Authority.

Home Organization: The organization with which an End User is affiliated. It is responsible for authenticating the End User and managing End Users' digital identity data.

Identity Management: Process of issuing and managing end users' digital identities.

Identity Provider (IdP): The IdP authenticates members of a home organization against an existing identity management system and providers and makes assertions on what attributes should be relayed to a service provider.

Interfederation: Voluntary collaboration of two or more Identity Federations to enable End Users in one Identity Federation to access Service Providers in another Identity Federation.

Service Provider: An organization that is responsible for offering the End User the service he or she desires to use. Service Providers may rely on the authentication outcome and attributes that Home Organizations and Attribute Authorities assert for its End Users.

4 Introduction

An Identity Federation (Federation) is an association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions.

The MAREN Identity Federation (MIF) is introduced to facilitate and simplify the introduction of shared services across the Federation. This is accomplished by using Federation Technologies to extend the scope of a digital identity issued by one Federation Member to be valid across the whole Federation. The Federation relies on Home Organizations and Attribute Authorities to correctly and accurately assert information about the identity of End Users to Service Providers, that may use that information to grant (or deny) access to the services and resources they offer to End Users.

The Federation Policy document defines the Federation by defining the Federation Members' obligations and rights to be able to use available Federation Technologies for electronic identification and for access to attribute and authorization information about End Users in the Federation. The Federation Policy also defines the obligations and rights of the Federation Operator. This document, together with any documents referred to herein, constitutes the Federation Policy.

5 Governance

5.1 Governance and Roles

The Malawi Research and Education Network (MAREN) hereafter referred to as the "governing body" or "MAREN", is entrusted with the governance of the Federation. In addition to what is stated elsewhere in the Federation Policy the governing body is responsible for:

- Setting membership selection criteria for the Federation.
- Granting or denying an application for membership in to the Federation.
- Revoking the membership if a Federation Member breaches the Federation Policy.
- Maintaining formal ties with relevant national and international organizations.
- Approving changes to the Federation Policy. Addressing financial needs of the Federation.
- Deciding on any other matter of interest to the Federation e.g. Whether or not members will be required to pay registration fee.

5.2 Obligations and Rights of Federation Operator

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator (i.e. Malawi Identity Federation) is responsible for:

- Secure and trustworthy operational management of the Federation and providing central services following the procedures and technical descriptions specified in this document.
- Provides support services for Federation Members' appropriate contact persons to work out operational problems regarding the Federation services.
- Acts as a centre of competence for Identity Federation: tests software, recommends and documents solutions, provides software deployment and

configuration guides for selected software and operating systems for use within the Federation.

- Prepares and presents issues to MAREN and acts as the secretary of the MAREN meetings.
- Maintaining relationships with national and international stakeholders in the area of Identity Federations. This especially includes contacts regarding interfederation activities and work with other Identity Federations in the area of harmonization.
- Promoting the idea and concepts implemented in the Federation so prospective Federation Members learn about the possibilities of the Federation.
- Where applicable, the Federation Operator will be responsible for the implementation of Data Protection Compliance Requirements for the Federation in line with the applicable Data Protection laws and regulations.

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator reserves the right to:

- Temporarily suspend individual Technology Profiles for a Federation Member that is disrupting secure and trustworthy operation of the Federation.
- Publish a list of Federation Members along with information about which profiles each Federation Member fulfills or implements, for the purpose of promoting the Federation.
- Publish some of the data regarding the Federation Member using specific Technology Profile. Definition of which data may be published is provided in appropriate Technology Profiles.

5.3 Obligations and Rights of Federation Members

In addition to what is stated elsewhere in the Federation Policy, all Federation Members:

- Shall appoint and name an administrative contact for interactions with the Federation Operator.
- Must cooperate with the Federation Operator and other Members 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 its members.
- Must comply with the obligations of the Technology Profiles which it implements.
- Must ensure its IT systems that are used in implemented Technology Profiles are operated securely.
- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws and regulations thereunder and must comply with the Standard Data Protection Policy developed by the governing body or their own Data Protection Policy that has been approved by the governing body.

If a Federation Member is acting as a Home Organization, it:

- Is responsible for delivering and managing authentication credentials for its End Users and for authenticating them.
- Should submit its Identity Management Practice Statement to the Federation Operator, who in turn makes it available to other Federation Members upon their request. The Identity Management Practice Statement is a description of the Identity Management life-cycle including a description of how individual digital identities are enrolled, maintained and removed from the identity management system. The statement must contain descriptions of administrative processes, practices and significant technologies used in the identity management life-cycle, which must be able to support a secure and consistent identity management life-cycle.

- Ensures an End User is committed to the Home Organization's Acceptable Usage Policy.
- Operates a helpdesk for its End Users regarding Federation services related issues.

Home Organizations are encouraged to maintain a helpdesk for user queries at least during normal office-hours in the local time zone. Home Organizations must not redirect End User queries directly to the Federation Operator, but must make every effort to ensure that only relevant problems and queries are sent to the Federation Operator by appropriate Home Organization contacts.

If a Federation Member is acting as a Home Organization or Attribute Authority, it:

- Is responsible for assigning Attribute values to the End Users and managing the values in a way which ensures they are up-to-date.
- Is responsible to releasing the Attributes to Service Providers.

If a Federation Member is acting as a Service Provider, it:

- Is responsible for making decision on which End Users can access the services they operate and which access rights are granted to an End User. It is the Service Providers' responsibility to implement those decisions.

6 Eligibility

The Federation sets out eligibility criteria that determines who is able to become a Federation member. The responsibility for setting membership criteria rests with MAREN and may be revised from time to time. Any institution that qualifies to be a member of MAREN also qualifies to become a member of MIF (the Federation). The MAREN Federation membership criteria are fully described on the MIF website https://mif.maren.ac.mw.

7 Procedures

7.1 How to Join

- In order to become a Federation Member, an organization applies for membership in the Federation to MAREN by agreeing to be bound by the Federation Policy. This is done in writing by an official representative of the organization.
- Each application for membership including (if applicable) the Identity Management Practice Statement is evaluated by the Federation Operator. The Federation Operator presents a recommendation for membership with an evaluation report to MAREN who in turn decides on whether to grant or deny the application.
- If the application is denied, this decision and the reason for denying the application are communicated to the applying organization by the Federation Operator.
- All Federation Members shall be bound by this Federation Policy (and any other documents referred to herein).

7.2 How to Withdraw

- A Federation Member may cancel its membership in the Federation at any time by sending a written request to the Federation Operator. A cancellation of membership in the Federation implies the cancellation of the use of all federations Technology Profiles for the organization with immediate effect. The Federation Operator may cancel its participation in the Federation by announcing the termination date to the Federation Members. Until termination date, Federation Operator shall run the Federation on best effort basis. After the termination date, Federation Operator shall cancel the use of all Federations Technology Profiles for all Federation Members.

8 Legal conditions of use

8.1 Termination

- If a Federation Member does not follow the Federation Policy, their membership in the Federation may be canceled.
- If the Federation Operator is aware of a breach of the Federation Policy by a Federation Member, the Federation Operator may issue a formal notification of concern. If the cause for the notification of concern is not rectified within the time specified by the Federation Operator, the governing body may issue a formal notification of impending revocation after which the governing body can decide to revoke the membership should the said Federation Member fail to comply or rectify the breach.
- Revocation of a membership implies the revocation of the use of all Technology Profiles for the Federation Member with immediate effect.

8.2 Liability and indemnification

- The Federation Operator offers this service on an “as is” basis, that is, without liability for Federation Operator and MAREN for any faults, losses, damages, errors and defects meaning, amongst other, that the Federation Member cannot demand that the Federation Operator or the governing body amends defects, refunds payments or pay damages. By accepting membership to the Federation and agreeing to be bound by the Federation Policy, each Federation Member (and End User) agrees that the governing body and the Federation Operator shall not be liable for any errors, damages or losses and that each Federation Member accepts liability for its reliance on the information or data provided in the Federation. The Federation Operator will nevertheless strive to ensure that any faults and defects of significance are corrected within a reasonable period. Further, the Federation

Operator will endeavor to put in place sufficient technical, organizational, and structural measures that are reasonably proportionate to the potential risks that the Federation faces.

- The Federation Operator and MAREN shall not be held liable for any loss, damage or cost that arises as a result of the Federation Member connection to or use of Federation services, or other systems to which the Federation Member obtains access in accordance with this Policy.
- This limitation of liability does not however apply in the case of gross negligence or intentional fraudulent act shown by Federation Operator personnel.
- Neither the Federation Operator nor MAREN shall be liable for damage caused to the Federation Member or its End Users. The Federation Member shall not be liable for damage caused to the Federation Operator or MAREN due to the use of the Federation services, service downtime or other issues relating to the use of the Federation services.
- Unless agreed otherwise in writing between Federation Members, the Federation Member will have no liability to any other Federation Member solely by virtue of the Federation Member's membership of the Federation. In particular, membership of the Federation alone does not create any enforceable rights or obligations directly between Federation Members.
- Federation Operator and the Federation Member shall not claim damages from other Federation Members for damages caused by the use of the Federation services, service downtime or other issues relating to the use of Federation services. The Federation Member may, in its absolute discretion, agree variations with any other Federation Member to the exclusions of liability. Such variations will only apply between those Federation Members.
- The Federation Member is required to ensure compliance with applicable laws. Neither the Federation Operator nor MAREN shall be liable for damages caused by

failure to comply with any such laws on behalf of the Federation Member or its End Users relating to the use of the Federation services.

- Neither party shall be liable for any consequential or indirect damage.
- The Limitation of liability for acts or omissions shall not extend to offences under any written law and the offending party will be held individually liable unless the offence was in connivance with another party.
- Without prejudice to the limitation of liability under this clause, parties are under obligation to take necessary and reasonable measures with respect to their express and implied obligations.
- Neither the existence of interfederation agreements, nor the exchange of information enabled by it, shall create any new legal obligations or rights between Members or operators of any Federation, except as otherwise advised by the Federation Operator. Federation Operator and Federation Members remain bound only by their own respective laws and jurisdictions.
- The Federation Member and Federation Operator shall refrain from claiming damages from entities in other federations involved in an interfederation agreement.

8.3 Jurisdiction and dispute resolution

- This Federation Policy shall be governed by and construed in accordance with the laws of the Republic of Malawi.
- Should any dispute arise between the Parties hereto with regard to the interpretation, rights, obligations, and/or implementation of any one or more provisions of this Federation Policy, the Parties shall in the first instance attempt to resolve such dispute by amicable negotiation between themselves.

- If the issue cannot be resolved through negotiation, or if such negotiations do not succeed within four weeks of the date on which the claim for negotiations was made in writing by one party, the disputes shall be submitted, by either party, in writing (with a copy to the other Party) to the Centre for Litigation and Dispute Resolution, Republic of Malawi, who will appoint an arbitrator. If any provision of the Federation Policy is held to be unenforceable by any court of competent jurisdiction, such term or provision or part shall to that extent be deemed not to form part of this Federation Policy. The validity and enforceability of the remainder of this Federation Policy shall not be affected.

8.4 Interfederation

- The Federation may participate in interfederation agreements to encourage collaboration across national and organizational borders. The relevant Technology Profiles outline how the possible interfederation agreement is administratively and technologically expressed for specific technologies.
- The Federation Member recognizes and knows that through those interfederation agreements, the Federation Member may deal with entities that are bound by and committed to foreign laws and federation policies. Those laws and regulations may differ from those of this Federation.

8.5 Amendment

- The Federation Operator has the authority to alter the Federation Policy at any moment. Any such changes must be authorized by the governing Body and must be reported in writing to all Federation Members at least 90 days prior to their implementation (before they take effect).