Lebanese Identity Federation Ecosystem (LIFE)

# Home Organization Acceptable Use Policy (AUP)

| | |
|---|---|
| **Policy Owner** | American University Of Beirut |
| **Related Policies** | LIFE Identity Federation Policy |
| **Effective Date** | January 2017 |

# Table of Contents

## 1. Overview

The Home Organization Acceptable Use Policy is a large and far-reaching policy that communicates to Home Organizations' users how the federation and the network services may be used. It covers such areas as personal use of communication, blogging, excessive use, information sharing, monitoring, copyright infringement, prohibited activities, and much more.

## 2. Purpose

This Policy communicates to the Home Organizations' users how to use the federation and the network services in a secure, appropriate, and legal manner in which they can make use of information and services offered in LIFE. An AUP will provide risk reduction by educating users on the federation's expectations and compliance requirements as well as clearly defining user standards for acceptable use of its services and network.

## 3. Scope

This Acceptable Use Policy (AUP) applies to the use of all information and services by LIFE members, service providers and end users. All Home Organizations' users should be aware of the legal obligations and internal policy in respect of information handling and services utilization.

This policy is a living document that will change as services structure or use changes in the federation.

All LIFE users are expected to have knowledge of at least the portions of this document that are directly related to their role within their Home Organization as a Federation Member.

## 4. Policy

1. The primary responsibility for determining changes to the AUP belongs to the Federation Executive Board.

2. The use of LIFE services is limited to activities related to the mission of the federation, including research, academic services and patient care.

3. Appropriate Use of Communication Channels

   ❖ Communication channels (e-mail, blogs, instant messaging, etc.) will not be used for intentional receipt and/or distribution of offensive material. There is a legal requirement for the Home Organization to handle any violation and to take appropriate preventative action.

   ❖ LIFE services must not be used for the creation, transmission, or deliberate reception of any material that is designed or likely to cause offence or needless anxiety, or is abusive, sexist, racist, defamatory, obscene, or indecent. When communicating electronically, users are expected to conduct themselves in an honest, courteous, and professional manner.

4. Confidentiality of Data

❖ All users, who have access to LIFE services are responsible for using it in accordance with the rules within this policy. In particular, all users must ensure that they use systems, information and services in such a way that they ensure patient, users and organizational confidentiality is maintained.

❖ All users are expected to respect the privacy of others by refraining from inspecting, broadcasting, or modifying personal data files without the consent of the individual or individuals involved.

❖ All end users are responsible for ensuring that classified and sensitive information is stored securely and that appropriate confidentiality is maintained when handling information.

5. Copyright Infringement

❖ Forging any other electronic message, or sending communication from any account other than your own without permission may be treated as fraud.

❖ Infringement of copyright by copying or transmitting copyright material without permission of the copyright holder ("fair use" notwithstanding) is strictly forbidden.

6. Security Controls

❖ A Federation Member is responsible for ensuring that any of services and systems can meet leading the minimum risk management practices and security requirements. Compliance also requires that end users are aware of their responsibilities.

❖ To restrict the possibility of viruses being transmitted to the network, users must not use their own computer for federation related activities unless anti-virus software and a firewall have been installed and are regularly updated.

❖ The Federation Member is responsible to ensure secure access facilities. Access restrictions to databases or systems containing important, classified and sensitive information is assumed to be protected by additional security controls by the system/data owner.

▪ Attempting to remove or bypass any security access is strictly forbidden.
▪ Users are required to protect their usage against loss, damage, or theft and against possible misuse by others. If a breach of security is recorded, the burden of proof will be with the registered user to show that they are not responsible for the breach.
▪ Users should report any known or suspected breaches of information security to their Home Organization.

7. Monitoring and Privacy

- ❖ Usage logs are performed on all backbone systems/services and global statistical data is disseminated via the appropriate media/channel where needed.
- ❖ The federation services activities will be monitored by authorized individuals for purposes of maintaining system performance and security. In instances when abuse an individual is suspected, the case will be reported to the Home Organization Administration for appropriate actions.

- ❖ Access to read logs and audit trails will only be granted to the Federation Operator authorized staff responsible for investigating system failure or misuse, and then only to look at information as necessary to repair or protect the systems/services or to investigate use that may be in contravention of this AUP.

8. Use for Illegal Activities

- ❖ Only licensed software and legally obtained data can be used in the federation activities in compliance with the license/purchase agreements and copyright/intellectual property laws. This includes all software packages, software upgrades, and add-ons. Violating the license agreement or making illegal copies of a software will be strictly treated as fraud.

9. Network Access

- ❖ Users are expected to enter the network only through an authorized digital identity granted by their Home organization/Federation Member.

10. Unacceptable Use

- ❖ Deliberate activities with any of the following consequences (or potential consequences) are prohibited:
  - ▪ Corrupting or destroying other users' data.
  - ▪ Using systems/services in a way that denies service to others.
  - ▪ Gaining access to systems that you are not authorized to use.
- ❖ Use or create invasive software, such as worms or viruses.
- ❖ Use LIFE channels to act in what may be perceived of as an obscene or harassing manner
- ❖ Forgery or other misrepresentation of one's identity via electronic or any other form of communication is a Fundamental Standard violation. Prosecution under State and Judicial body may also apply.

## 5. Enforcement

Failure to abide by this code may result in temporary or permanent dismissal of membership in LIFE and in actions being taken by the appropriate Administrative or Judicial body. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Discontinuity of membership
2. Legal action according to applicable laws and contractual agreements

## 6. Definitions

| | |
|---|---|
| End User | Any natural person affiliated to a Home Organization, e.g. such as an employee, researcher or student making use of the service of a Service Provider. |
| Federation | Identity 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. In this case the American University of Beirut (AUB) |
| 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. |
| 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. |
| Federation Executive Board | It is the decision making authority in the Federation Operator |