General LOFAR Systems User Access Policy

Draft 0.2
April 19, 2012

Introduction:

This document contains the general policy for usage of LOFAR ICT systems by all users (employed by/for LOFAR as well as external users that have access to LOFAR ICT Systems).

Definitions:

- LOFAR Observatory: For this document, the LOFAR Observatory is to be understood to be the organisation that is responsible for the operation and maintenance of the LOFAR International and Dutch telescopes. At the moment of writing this responsibility lies with the ASTRON Radio Observatory.
- System: any kind of ICT system. This includes, but is not limited to: computers, network systems (routers, switches, etc.), and printers.
- LOFAR Systems: Systems that are owned or operated by LOFAR as well as any part/functionality of third party systems that has been allocated to use by LOFAR.
- Terminal: a system used as a user interface to obtain access to LOFAR Systems.
- GUAP: The General LOFAR Systems User Access Policy.
- User: a person that has access to LOFAR Systems.
- System manager: a user that is authorized to manage one or more LOFAR systems. In general, this is associated with being able to monitor, access, and control all activities of users that have access to the managed systems.
- System access manager: a person that is authorized to approve and retract access to one or more LOFAR systems.
- Security officer: a person that is authorized to act on behalf of LOFAR in matters of LOFAR Systems security.
- LSSIRT: The LOFAR Systems Security Incident Response Team. A team of persons who are authorized to deal with security breaches on LOFAR Systems.
- Access level: The level of access to LOFAR Systems, determined by the user's role and function related to LOFAR. The following levels are considered:
    - Scientist
    - Operator
    - Commissioner
    - Developer
    - Administrator
    - System Manager
- Scope: The LOFAR systems that the user is granted access to. For example: CEP cluster; WAN infrastructure; international station system(s).

LOFAR Systems general policy:

The primary purpose of the LOFAR Systems is to enable effective and efficient operation of the Dutch and International LOFAR telescope. It is the responsibility of the LOFAR Observatory to operate and manage the LOFAR Systems such that the primary purpose is achieved as well as to assure that LOFAR Systems are only used for activities that are in line with the overall objectives and responsibilities of LOFAR. This includes taking measures to prevent unauthorized or illegal use of LOFAR.

To achieve these goals, the following general rules apply to the usage of LOFAR Systems:

- There shall be no usage of LOFAR Systems that hinders or disables effective or efficient operation of the International or Dutch LOFAR telescope.
- Users of LOFAR Systems are to be aware of their responsibilities
- Measures are to be taken to prevent unauthorized access to, and unauthorized use of, LOFAR Systems.

All users of LOFAR Systems should be aware of the latest version of the GUAP. This is ensured by:

- Include a GUAP statement in the welcome message of the Lofar portals, together with a pointer to the current GUAP document location.
- Publishing the latest version of the GUAP at a location accessible by all users.
- Notifying users whenever a new version of the GUAP is published.

User responsibilities:

Users of LOFAR Systems should realize they are not the only users of these systems. Many systems are multi-user systems and/or have a critical function in the operation of the LOFAR telescope. Together, the users of the LOFAR Systems form a community. Therefore, comparable to other shared infrastructures (e.g. traffic), the ground-rule on which this GUAP is based is that users may not endanger LOFAR Systems, nor may they hinder other users.

The above statement implies amongst other things that LOFAR users are not allowed to

- use the LOFAR Systems for other purposes than those related to the objectives of the International or Dutch LOFAR telescope,
- to undertake activities that will negatively influence operations of the LOFAR telescope or hinder other users in their LOFAR related activities,
- to try to obtain security information, such as passwords, from other users or systems.

The following paragraphs provide more detailed policies that users are to comply with. Even if none of these policy rules apply, users are expected to act in the spirit of the ground-rule above and the LOFAR Observatory may take appropriate action if this is not the case.

Privacy of accounts

Access to LOFAR Systems is only granted to individuals. Using other people's accounts or access-rights, or allowing third parties to use one's accounts or access-rights, will result in the discontinuation of one's account.

Attempts to gain initial access to LOFAR Systems using an account that is not registered to belong to an individual will be considered as attempted unauthorized access. Once having gained access to a LOFAR system using one's personal account, users may be authorized to access LOFAR Systems using non-personal accounts.

Copying software

Software made available on LOFAR Systems may be used subject to applicable licenses and copyrights. Any software stored on LOFAR Systems may not be copied for use elsewhere, unless explicit and written permission was granted by proper authorities. Conversely, installation and use of software on LOFAR Systems in violation of applicable licenses and copyrights is not allowed.

Using the LOFAR Systems

Use of LOFAR Systems, including hardware, software, network facilities and any information stored on the systems, is only allowed in accordance with the nature (access level and scope) of the provided account. Use of LOFAR Systems is always limited to LOFAR related activities. Any commercial use of LOFAR Systems is not allowed, unless explicit and written permission has been granted by appropriate authorities.

Users are responsible for illegal activities undertaken using the user's account irrespective of whether these activities are undertaken

- by the user him or herself,
- with consent of the user,
- or the result of the user not having taken appropriate measures to protect security related information.

Access to LOFAR Systems is to be traceable. Attempts to gain access to LOFAR Systems from or via non-traceable systems (e.g. anonymizers and systems/domains that are known or suspected to be compromised) will be treated as a potential threat. Attempted access from or via systems that are known or suspected to be used for illegal or abuse activities will be treated as a threat as well.

Protecting security information

By obtaining security information (e.g. account names, passwords, security tokens) third parties may gain access to LOFAR Systems. Even in this case, the registered user of that account is liable for any access or abuse of the LOFAR Systems. In order to minimize the probability that unauthorized parties obtain access to security information users are expected to adhere to the following guidelines:

- Keep access information secret. Do not hand this information over to friends or acquaintances.
- Do not type your password when someone can see what you are typing.

- Do not store security information (e.g. passwords, keys and certificates) in a place, or send it over a network, that cannot be trusted to be private and secure.
- If keys or certificates are used to access LOFAR systems, the secret/private files are to be protected by a safe password (see below) and they are to be stored such that they are only accessible by the owner (e.g. on linux systems chmod 700 on the containing directory and chmod 600 on the secret file). As few copies as possible are to be stored, preferably not more than one.
- Do not leave terminals unattended that have an open session from where the user is logged in on a LOFAR system. Either log out of all LOFAR Systems or secure the session with a safe password before leaving the terminal.
- Change passwords every now and then. Opinions differ about the optimal interval for password changes, but experts in the field of security advocate to change passwords at least once a year.
- Do not use a password that is, or has been, used on insecure or untrusted systems or that has been sent across an insecure or untrusted network. For example, do not use a password that has been used for an account on a commercial, social, or private website.
- Do not use personal data or information, or that of friends or relatives, when constructing a password.
- Do not use existing words or abbreviations as a password or any string that is known to have been published.
- Use at least one character from each of the following characters when constructing a password:
    - Lower case characters from the alphabet
    - Upper case characters from the alphabet
    - Digits (0-9)
    - Punctuation characters
- Use at least 8, and preferably 12, characters for passwords.
- Easy to remember, but hard to guess, passwords can be constructed by taking a sentence and use only the first character of each word, replacing some words or characters by digits and punctuation characters. For example (do not use this for real as it now is published strings!!!):
    - `LOFAR is a unique and awesome instrument looking up at the sky`: L1au&ail^@ts

Reporting security issues

All multi-user systems are vulnerable to security breaches. If the user finds a flaw in a system’s security setup this should be reported to the LOFAR security officer. It is not allowed to exploit a weakness in the security setup of LOFAR Systems. By reporting the weakness, users effectively help to optimize the reliability of LOFAR systems and potential misunderstandings about intentions and suspected unauthorized activities of the user will be prevented.

If a user has indications that private security information is no longer exclusively known to, or accessible by, the user, this fact, plus the suspected time since when this situation has occurred, is to be reported immediately to the LOFAR security officer and the user is to replace/change private security information at the first possible moment.

If a user has indications that someone has obtained unauthorized access to LOFAR Systems or that illegal or unauthorized activities are undertaken using LOFAR Systems, this fact is to be reported immediately to a member of the LOFAR Systems Security Response Team.

Abuse of privileges and/or LOFAR Systems

Abusing LOFAR Systems may result in disciplinary action.

Abuse of LOFAR Systems and privileges is illustrated by, but not restricted to, the following examples. Users of LOFAR Systems are expected to prevent and fight any abuse of the LOFAR Systems in the spirit of this GUAP. The examples are provided for illustration only and are not to be considered as an exhaustive list.

It is not allowed:

- To initiate massive data transfers from or to LOFAR Systems without prior consent from the LOFAR Observatory. In particular, it is not allowed for a user to copy large (more than a gigabyte) LOFAR dataset files other than via data transfer services supported by the LOFAR Observatory (data access policy?).
- To modify or to replace hardware or software without having obtained prior permission from proper authorities.
- To use LOFAR Systems, or any software or data stored on LOFAR Systems without having obtained prior permission from proper authorities.
- To use LOFAR Systems for non-work related activities for accessing or maintaining websites, social network sites, internet banking, etc.
- To send any messages using other people's names and/or addresses, or to read or distribute other people's messages without having obtained their prior consent.
- To alter IP addresses or other identifying data of LOFAR Systems (e.g. by using spoofing).
- To attempt to obtain unauthorized access from LOFAR Systems to other systems or to non-public data or resources inside and outside the LOFAR network.
- To distribute or make available obscene, aggressive, discriminating, unethical, or threatening information.

In case there are strong indications that LOFAR Systems are, or have been, abused and the abuse can be traced down to a personal account, the following actions shall be taken to ensure the safety and integrity of the LOFAR Systems:

- The authorizations associated with the suspected account may be restricted or suspended, awaiting the results of further investigation.
- System management may be ordered to inspect the contents of information stored in, sent by or sent to that account (see also the section on system manager responsibilities).
- The user associated with the account will be notified.
- If the abuse is found to have resulted in damage to LOFAR Systems or any other damage, the user associated with the account will be held liable. Appropriate measures will be taken which may include demanding compensation of the user, reporting the case to the employer of the user and/or reporting the case to the authorities.

System manager responsibilities:

System managers have the same rights and duties as other users of LOFAR Systems. However, the authorization level related to their positions leads to additional security related requirements. System managers are responsible for:

- Managing personal user accounts, and authorizations linked to those accounts, to enable authorized activities on LOFAR Systems.
- Managing access to non-personal accounts, and authorizations linked to those accounts, to enable authorized activities on LOFAR Systems.
- Ensuring that the users of the LOFAR Systems have access to the software and hardware as required by the users to perform their tasks related to LOFAR. Requests for the installation of software should always be considered conditional to the intended function of a LOFAR system. For example, webservices will in general not be installed on a system that is not intended to serve (web) content.
- The security of LOFAR systems themselves, including the installation and proper maintenance of appropriate software in cooperation with the security officer.
- Monitoring and analyzing in- and outbound network traffic to uphold and maintain system security and integrity.
- Destroying collected network traffic information after at most six months unless law requires longer or shorter retention times in which case the minimum legal retention time will be applied.
- Analyzing collected network traffic information for the presence of malware like viruses, Trojan horses and worms.
- Taking measures to prevent unauthorized user access to LOFAR systems.
- Supporting system access managers, the security officer and the SRRT in carrying out their respective tasks.
- In case of incidents, restoring systems and services when the incident has been resolved.

System managers have access to confidential and private information. They are as such required:

- To consider any information about the LOFAR Systems as well as any information stored in the system, in particular if stored using a personal account, as confidential.
- Not to perform any content inspection or analysis of information within the LOFAR Systems unless there is a clear indication that the owner or originating user account is used for abuse or illegal purposes and only after having received an authenticated order to do so from the director of the LOFAR Observatory.
- If required, for example for security scans, and only following an authenticated order from the director of the LOFAR Observatory, to collect and submit for further investigation specific information (e.g. data or software) in order to solve any problems that were encountered using the data and software.

System access manager responsibilities:

LOFAR System access managers are authorized to grant and deny access of users to certain LOFAR Systems. More detailed User Access Policies for those systems specifically may apply. A list of System Access managers, and the LOFAR Systems each system access manager is authorized to grant or deny access to, is maintained by the LOFAR Observatory and can be found on the Lofar operations wiki: http://www.lofar.org/operations/doku.php?id=operator:ilt_to_contacts

Security officer responsibilities:
The LOFAR Security officer is responsible for the realization of security related policies and maintains an administration of LOFAR Systems Usage Agreements. The officer drafts policy documents and brings them to the attention of all users.

The officer is authorized to take decisions on security related issues concerning LOFAR Systems that are not time critical, when such an issue is not addressed in a formalized policy.

If there is a dispute about a security related decision made by the security officer, the dispute will be put before the director of the LOFAR Observatory who will take a final decision in the matter. The original decision remains in effect until the director of the LOFAR Observatory has ruled otherwise.

LSSIRT responsibilities:
The LOFAR LSSIRT is responsible for dealing with time critical computer security related incidents (hacks/abuse/denial of service). The tasks of this team are purely reactional. The team is authorized to disable any LOFAR system or service as needed to avoid further damage.

If any illegal activity is detected on LOFAR Systems, the LSSIRT is to be alerted immediately. Contact information can be found at http://www.lofar.org/operations/doku.php?id=public:securityresponseteam .

The team will then:

- Investigate the incident
- Take inventory of the damage
- Gather evidence
- Stop the illegal activity
- Advise system managers on how to prevent similar illegal activities in the future (system/service restoration is also left to system managers)
- Communicate with LOFAR Observatory management, and with appropriate external authorities if authorized to do so by LOFAR Observatory management.
- Communicate with managers of infrastructures around the LOFAR network (e.g. ASTRON/SurfNet/RUG/Sara)
- Report the incident, and the actions taken, to LOFAR Observatory management.

The team will use a structured approach for each incident. If needed, this approach will be updated regularly to create a best practice for the operation of LOFAR Systems.

LOFAR Observatory responsibilities:

The LOFAR Observatory:

- Is responsible for the management and operation of the LOFAR Systems.
- Formalizes policies related to LOFAR Systems.
- Authorizes persons to take the role and responsibilities of system manager, system access manager, security officer or LSSIRT member and keeps an administration of these authorizations.

- Manages and operates LOFAR Systems in such a way that users can fulfil the tasks and activities that are expected from them.
- Manages the usage of LOFAR System resources (e.g. compute cycles, storage capacity)
- Takes action in case of illegal or unauthorized access to LOFAR Systems
- May report illegal use of LOFAR Systems to the appropriate authorities, in particular when the illegal use resulted in damage to LOFAR or third party systems or interests.