

# INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME



Large Scale Monitoring of Broadband Internet Infrastructure  
Contract No. 004336

## **D0.2 “Acceptable Use Policy for the Fair Sharing and Use of the Infrastructure”**

**Abstract:** This document presents the need for an acceptable use policy (AUP) for LOBSTER infrastructure, a short review of AUPs for similar systems, the results from the answers on AUP related questions in LOBSTER questionnaire and a proposed AUP document for LOBSTER.

|                                     |                 |
|-------------------------------------|-----------------|
| <b>Contractual Date of Delivery</b> | 31 May 2005     |
| <b>Actual Date of Delivery</b>      | 31 May 2005     |
| <b>Deliverable Security Class</b>   | Public          |
| <b>Editor</b>                       | FORTHnet        |
| <b>Contributors</b>                 | FORTHnet, FORTH |

The LOBSTER Consortium consists of:

|           |                      |                 |
|-----------|----------------------|-----------------|
| FORTH-ICS | Coordinator          | Greece          |
| VU        | Principal Contractor | The Netherlands |
| CESNET    | Principal Contractor | Czech Republic  |
| UNINETT   | Principal Contractor | Norway          |
| ENDACE    | Principal Contractor | United Kingdom  |
| Alcatel   | Principal Contractor | France          |
| FORTHnet  | Principal Contractor | Greece          |
| TNO       | Principal Contractor | The Netherlands |
| TERENA    | Principal Contractor | The Netherlands |



## Contents

|  |           |
|--|-----------|
| <b>1 Introduction .....</b>  | <b>3</b>  |
| <b>2 The Motivation for an Acceptable Use Policy for LOBSTER infrastructure.....</b> | <b>4</b>  |
| <b>3 Similar infrastructures AUP review .....</b>                                    | <b>5</b>  |
| <b>4 AUP requirements collection and analysis .....</b>                              | <b>9</b>  |
| <b>5 Proposed AUP document .....</b>   | <b>15</b> |
| <b>6 AUP administration .....</b>  | <b>17</b> |
| <b>A1 LOBSTER Questionnaire – PART D.....</b>  | <b>19</b> |
| <b>A2 Similar Infrastructures.....</b>   | <b>22</b> |



## 1 Introduction

LOBSTER is an advanced pilot European passive Internet traffic monitoring infrastructure that will improve our understanding of the Internet and will contribute towards solving difficult performance and security problems. Based on appropriate abstractions and willing-full cooperation among points of presence, it will contribute towards effectively monitoring the underlying network, providing early warning for security incidents, and accurate and meaningful measurements of network performance.

The main goal of LOBSTER is to deploy an advanced pilot European Internet Traffic Monitoring Infrastructure based on passive monitoring sensors at speeds starting from 1 Gbps and possibly up to 10 Gbps.

Dissemination of the LOBSTER infrastructure will eventually lead to the collaborative sharing of the monitoring data and the infrastructure capabilities. For the smooth operation during this collaborative monitoring the definition of an Acceptable Use Policy (AUP) is necessary, in order to manage privacy and security issues. In the following sections, first we argue about the necessity of an acceptable by all participants use policy for LOBSTER infrastructure, then we review the AUP documents of similar infrastructures and we analyze the responses of the AUP related questions in LOBSTER questionnaire, which are presented in Section A1. Finally, based on the feedback obtained from the questionnaire, we define a document concerning the acceptable use of LOBSTER infrastructure.



## 2 The Motivation for an Acceptable Use Policy for LOBSTER infrastructure

LOBSTER is based on powerful monitoring methods collectively known as passive monitoring. Since passive monitoring methods record complete traffic information, they are able to tackle monitoring problems more effectively than other well-known monitoring methods (i.e. flow-level statistics, active monitoring, etc). Potential users of LOBSTER will eventually share the same infrastructure, so a fair and acceptable by all participants' policy, must be established, which will outline the acceptable use of LOBSTER's resources.

This policy is provided to guide and inform all potential users about what constitutes acceptable (i.e. permitted) use of LOBSTER's infrastructure. It does not intend to constrain users unnecessarily, but to provide all the appropriate means to the organizations in order to be able to enforce their policy concerning privacy and security of users activities inside the organization and also protect them against the consequences of any misuse of LOBSTER's infrastructure.



### 3 Similar infrastructures AUP review

On the Internet there are many examples of infrastructures installed at different places whose resources are shared among many users. Such examples are Grid computing and Supercomputers' networks. The participants of these infrastructures have defined general purpose rules and policies in order to achieve fair use of resources and the data they provide.

This section presents short reviews on documents regarding acceptable use policy on such infrastructures.

#### a. PlanetLab

PlanetLab is an overlay testbed designed to allow researchers to experiment with network applications and services that benefit from distribution across a wide geographic area. It consists of computational resources hosted by organizations (principally research organizations like Universities) that donate their own time, rack-space, and network connectivity for the good of the community. Running an experiment on PlanetLab is fundamentally different from running it in a LAN-based lab or on an isolated wide-area test bed.

The main parts of the PlanetLab's AUP document and some of the regulations they introduce are the following:

- General guidelines
  - General guidelines for the proper operation of the system are mentioned.
- Overall rules.
  - PlanetLab should not be used for any illegal or commercial activities. Use of research and educational purposes are allowed.
- Node Usage Rules

Specific rules for the proper usage of PlanetLab nodes are described, such as:

- Use existing security mechanisms.
  - No hacking attempts of the PlanetLab nodes
  - Do not circumvent accounting and auditing mechanisms.
  - Avoid spin-wait for extended periods of time.
- Network Usage Rules



## Acceptable Use Policy for the Fair Sharing and Use of the Infrastructure IST-004336

Specific rules for the proper usage of PlanetLab network resources are described, such as:

- Do not use your PlanetLab slice (account) to gain access to any hosting site resources that you did not already have.
- Do not use one or more PlanetLab nodes to flood a site with so much traffic as to interfere with its normal operation.
- Do not do systematic or random port or address block scans.
- Consequences  
The most common consequences are mentioned such as, disabling the account and informing the organization's administrator.

### b. UK National Grid Service

The National Grid Service (NGS) is the core UK grid, constructed for academic research work and intended for the production use of computational and data grid resources. The NGS is the UK's first production level Grid for e-Science. It provides compute and data resource for UK academics and part of its remit is to encourage use of the e-Science Grid particularly by those academics who ordinarily would not have access to Grid type resources.

The main parts of the NGS' AUP document and some of the regulations they introduce are the following:

- Purpose of NGS AUP  
Describes the reasons why the specific AUP document is composed.
- Scope of NGS AUP
- Registering to use the National Grid Service  
Describes the processes one should follow in order to have access to the Grid.
- Regulations  
Specific rules for the proper usage of the Grid are described, such as:
  1. The regulations of the various Grid resources must be respected.
  2. Disruption of the Grid or any other system must not be attempted.
  3. Copyright legislation applies to software and data used.
  4. The terms of software and data licences must be respected.
- Enforcement  
Rules and directions for the enforcement of the Grid's policy are



## Acceptable Use Policy for the Fair Sharing and Use of the Infrastructure IST-004336

described, such as:

1. As a user, whenever you use the Grid, you are bound by all the above regulations and the legislation in force at the time.
2. The regulations and legislation which applies to you will be enforced by your own project.
3. Penalties will be levied for confirmed breaches of regulations.
4. All Grid institutions have agreed to co-operate in investigating disciplinary cases.

- Non – research use of Grid resources

The Grid has been constructed for academic research work only. If an organization wishes to use the Grid for any other purpose this must be authorized in a documentary form in advance by the leader/principal investigator of the project/virtual organization. They will be expected to provide detailed information in support of their requirement.

### c. JANET

JANET is an electronic communications network and a collection of electronic communications networking services and facilities that support the requirements of the UK higher and further education and research community.

The main parts of JANET's AUP document are the following:

- Background and definitions

This part provides useful background information and definitions about the network infrastructure used. Also, rules concerning the scope of the policy's document are mentioned:

- This policy applies in the first instance to any organization authorized to use JANET.
- JANET is maintained to support teaching, learning and research.

- Acceptable use

An organization may use JANET for the purpose of interworking with other organizations, and with organizations attached to networks which are reachable via interworking agreements operated by UKERNA. All use of JANET is subject to payment of the appropriate charges in force during the period of service. Any provision of service must be authorised in advance.



## Acceptable Use Policy for the Fair Sharing and Use of the Infrastructure IST-004336

- Unacceptable Use

This part contains detailed description for all unacceptable uses of JANET. It may not be used for any of the following:

1. the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
2. the creation or transmission of defamatory material
3. the transmission of material such that this infringes the copyright of another person
4. deliberate unauthorised access to facilities or services accessible via JANET

- Passing on and resaling JANET

Regulations concerning the passing on or resaling access to third parties.

- Compliance with the rules

It is the responsibility of the User Organisation to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of JANET does not occur. The discharge of this responsibility must include informing those at the Organisation with access to JANET of their obligations in this respect. Where violation of these conditions is illegal or unlawful, or results in loss or damage to UKERNA or JANET resources or the resources of third parties accessible via JANET, the matter may be referred for legal action.

### d. NSFNET - vBNS

The US National Science Foundation (NSF) has entered into a cooperative agreement with MCI Telecommunications Corporation to provide very high speed Backbone Network Service (vBNS). The vBNS will provide high bandwidth networking for research applications and will allow researchers to push the boundaries of networking research, ultimately developing technology and applications that are expected to benefit Internet users. The vBNS will only be available for meritorious high bandwidth users and will not be used for general Internet traffic.

In vBNS' AUP document it is clearly stated that it's services are provided to support research and education in and among US research and education institutions and for private or personal communication incidental to such activities. Use for other purposes is not acceptable. It describes the kind of institutions and organizations that can utilize its resources as well as the operations that each one may or may not perform.



## 4 AUP requirements collection and analysis

The data presented in this section, are the results of processing the responses on the AUP related questions in LOBSTER questionnaire. The goal of these questions was to investigate people's expectations of the LOBSTER infrastructure, their preferences, any existing constraints or rules that may restrict their participation in the project. Based on the input from the obtained responses, a use policy will be defined that will be fair to and acceptable by every participating institution.

There were eleven (11) questions in LOBSTER's questionnaire regarding AUP, while the total number of responses is twenty-three (23). The set of the questions processed can be found in section A1.

- Question: Data you could give to LOBSTER.

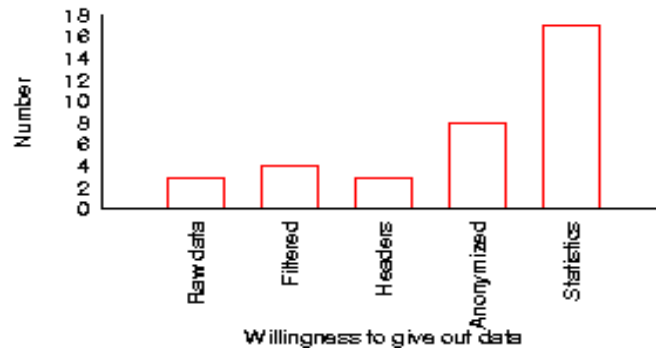


Figure 1: Data you could give to LOBSTER

Figure 1 indicates that only three out of twenty-three are willing to provide raw data; four out of twenty-three agree on providing filtered data, three of them agree on providing header information, eight on providing anonymized data and 14 on providing statistics. Overall, 13% is willing to give out full data, while 70% is reluctant and is willing to provide only statistics. All these indicate that potential users of LOBSTER will be able to access limited data disseminated by other users. Furthermore, they should not use the acquired data for purposes other than those specified by the provider.



- Question: Required Level of data anonymization?

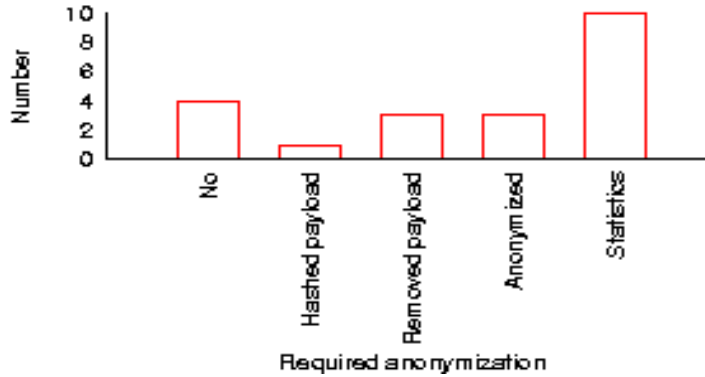


Figure 2: Required Level of Anonymization

Figure 2 shows that 13% of the participants would prefer to provide data with removed payload and full IP anonymization, 17% would prefer to provide data with no anonymization, 13% data with removed payload and light sanitized IP address and 9% data with hashed payload. These results indicate that the majority of the potential users would prefer to distribute processed data, removing any kind of information that could be considered sensitive. So, no-one should move proprietary data from the LOBSTER system, without the prior agreement of their owner, nor violate the security policy of other users in order to gain access to private information.

- Question: Expected output from LOBSTER?

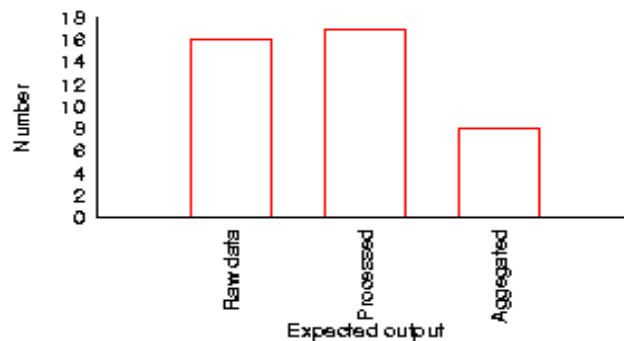


Figure 3: Expected output from LOBSTER System



Figure 3 indicates that 16 out of 23 potential users would prefer to get processed data as output from LOBSTER. 13 out of 23, would also like to get raw data for own processing. Since these data have been properly anonymized, they can safely be distributed. Finally, 7 out of 23 would also like to get aggregated data.

- Question: Issues that may restrict participation to project.

There are restrictions that LOBSTER participants have to take into consideration. Such restrictions are indicated below:

1. Laws on protection of privacy
2. Regulation of Investigation Powers
3. Military nodes on the network
4. Workload

Finally, there are cases for which further discussion is needed.

All these answers indicate that potential users of LOBSTER should respect any company, organization, national or EC regulations that may exist and not violate the security policies of other participants.

- Question: Sensitive data that limit your participation.

There are several cases of sensitive data that could limit one's participation in LOBSTER. Such limitations are indicated below:

1. Lots of data must be kept confidential
2. Only anonymized data can be provided
3. Only statistics can be provided
4. Restrictions on some nodes (military)

There are cases with no limitation on providing data (17 out of 23).

All these indicate the need for respect of users' privacy and existing regulations and also the need to retain useful information in data shared.

- Question: Acceptable usage of provided data.

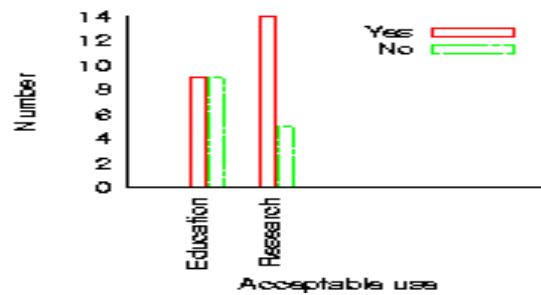


Figure 4: Acceptable usage of provided data

Figure 4 indicates that 14 out of 23 participants agree on using the provided data for research, while 9 of them do not agree on educational use of provided data. As a result, the disseminated data must not be used for purposes others than those agreed.

- Question: Available bandwidth to be used by LOBSTER.

The answers recorded are the following:

1. 1, 5, 10, 50 Mbps
2. Less than 1% of backbone links
3. In the order of Gbps (to be agreed)
4. Further discussion needed

These results indicate that potential users would not like their participation in LOBSTER to limit their bandwidth at any rate. Transmission of data that may cause annoyance to other participants or introduction of malicious programs into the infrastructure must be prohibited.

- Question: LOBSTER installation and problem solving.

Concerning installation and troubleshooting 11 out of 23 answered that they would prefer to deal with it manually while 6 to be done remotely. Concerning system failure and malfunction 7 out of 23 prefer to cooperate with other participants in the consortium for solving it, while 11 would prefer to have a centralized help desk available (Figure 5).

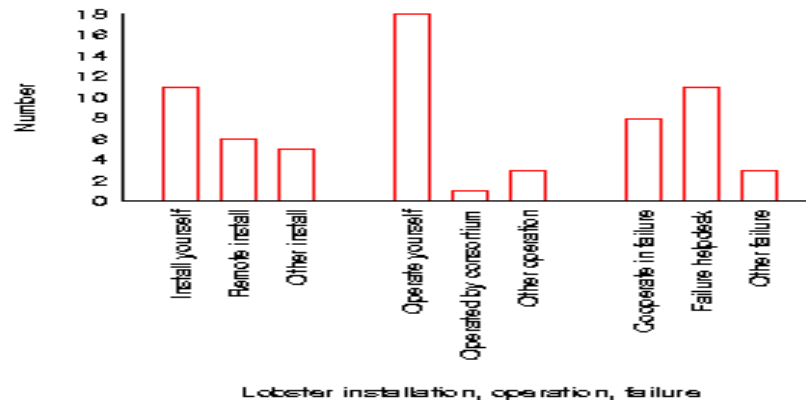


Figure 5: Course of Action (Installation, Operation, Failure)

- Question: Responsible for the LOBSTER Service operation.

All participants answered they would prefer to be in charge for the LOBSTER Service operation in their organization (Figure 5).

The previous two questions, indicate that users must not interfere with other participants' work, unless they are granted to do so. Unauthorized access to LOBSTER facilities or any other kind of disruption of a participant must be considered unacceptable.

- Question: Cooperation with LOBSTER.

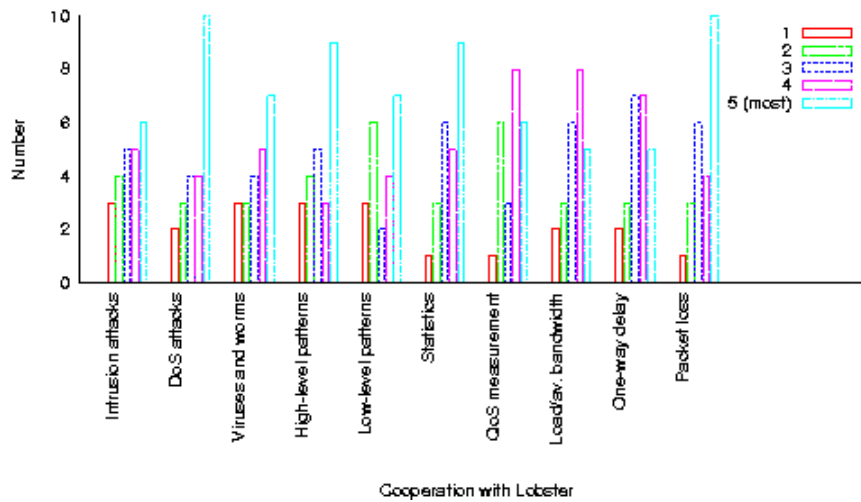


Figure 6: Cooperation with LOBSTER Activities

Figure 6 indicates that participants are primarily interested in collaborating within LOBSTER for estimating their packet loss rate. They are also very interested in dealing with DoS/DDoS attacks and in collecting statistics concerning their network traffic, as well as identifying high-level patterns and gathering QoS measurements.

As a result, the data provided by all LOBSTER users, could be used to detect cyber-attacks and in general support Internet-related research and security analysis.

The above questions mostly indicate that preferences and expectations from the LOBSTER infrastructure are varying among potential users. Most users would like to receive results both in a graphical representation (e.g. statistics) and as raw data. However, few people are willing to provide raw data related to their organization, to others. This is because people are generally afraid to distribute their data, unless they are absolutely sure that they will not be used for purposes other than the ones specified by the project targets.

As a result, respect for other users' work and privacy on the infrastructure, is very important for the proper operation of the infrastructure and cooperation among users. Every potential user must be certain that using the LOBSTER infrastructure will not cause any malfunction or other kind of annoyance to their network resources. Also, any national, European or company regulations concerning network activities that may exist should not be violated by potential users of LOBSTER infrastructure in any case.



## 5 Proposed AUP document

This section presents Acceptable Use Policy (AUP) for LOBSTER infrastructure. This AUP is based on the feedback that we received from the questionnaire answers and info retrieved from similar infrastructures' AUP. Future changes and updates of this policy, whenever needed, are possible as long as all participants agree. This policy is more a code of ethics rather than a legislation document. However, potential violations of this document may cause disciplinary actions against the offender.

### Overview

LOBSTER is an advanced pilot European Infrastructure for accurate Internet traffic monitoring. It is based on passive monitoring and aims to the improvement of people's understanding about the Internet and the solution of difficult performance and security problems.

All potential users of LOBSTER need to be aware of this document.

### Purpose of this document

The purpose of this policy is to outline the acceptable use of LOBSTER's resources. The regulations provided intend to protect all participating users, along with the organizations they come from, against the consequences of any misuse of LOBSTER's infrastructure.

### Scope

- a. This policy applies to every user of the LOBSTER infrastructure.
- b. This policy applies to the use of all LOBSTER's hardware resources, including monitoring sensors/adapters, communication lines and any other equipment and network facilities connected to the infrastructure.
- c. This policy applies to the use of all software within LOBSTER, all traffic data collected by the system and all project results disseminated.

### General Rules

- a. You are granted resources within LOBSTER in order to have access to network traffic monitoring data provided by all LOBSTER participants, that will be used to detect cyber-attacks, develop novel applications enabled by the availability of the passive network monitoring infrastructure, and in general support Internet-related research and security analysis. The information is not provided for any other purposes (e.g. for commercial use).
- b. You must respect any company, organization, national or EC regulations and policies referred to the use of network facilities.
- c. You must not violate any security/access policy of other participants.



**Acceptable Use Policy for the Fair Sharing and Use of the Infrastructure**      **IST-004336**

- d. You must immediately take the appropriate actions, when informed that some aspect of your LOBSTER sensor usage is creating a problem.
- e. In case accounts are created in the future in LOBSTER sensors or other LOBSTER infrastructure to possible users, they should select safe passwords and pass phrases, endeavor to keep them and their credentials secret and under no circumstances communicate them to third parties.
- f. You must not interfere with other participant's work.
- g. You must not attempt to disrupt the working of the LOBSTER infrastructure or attack against the system or any other participants.
- h. You must respect copyright legislation that applies to software and hardware used and to disseminated data.
- i. You must not move proprietary data to, from, or via the LOBSTER system without the prior agreement of their owner.
- j. You must not use disseminated data for commercial purposes and personal interest.
- k. Once you have registered to participate in LOBSTER, it is your responsibility to remain aware of the rules in this policy, including any changes made to them.
- l. You must not use LOBSTER's facilities to create or transmit material that may cause annoyance, inconvenience to other participants or any kind of malfunction to the system.
- m. Introduction of malicious programs into the infrastructure (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.
- n. Deliberate unauthorized access to facilities, services or data accessible via LOBSTER will be considered unacceptable.

**Enforcement**

- a. As a user of LOBSTER, you are bound to all of the above regulations.
- b. Ignorance of regulations or legislation is not a defense.
- c. Violation of this AUP may have several consequences for the offender.
- d. Penalties may be levied for confirmed breaches of regulations.
- e. LOBSTER Administration Committee (LAC) will review each case of LOBSTER AUP violation. Depending on the nature of the violation disciplinary action may be taken.



## 6 AUP administration

The rules in LOBSTER's AUP document apply to every potential user of the infrastructure. Potential users should respect and should not violate the policy's rules.

However, it is likely that violations of those rules may exist. For that reason, an AUP administration committee will be formed to handle and investigate any unacceptable use of the infrastructure.

The LOBSTER AUP administration committee will be composed of three (3) equivalent members, researchers and/or developers, who already cooperate in the LOBSTER project. The members will be designated by the partners of the consortium every two years.

The main responsibilities of the AUP committee will be the following:

- Rules enforcement

The AUP committee will be responsible for the enforcement of the AUP's rules on every user.

- Contact for complaints

The AUP committee will be responsible for monitoring for potential violation of LOBSTER's AUP. They will also be the point-of-contact for complaints about misbehaving usage of LOBSTER infrastructure. Every user that detects any case of misuse of the infrastructure, will be able to contact the committee via email at the email alias [lac@lobster.org](mailto:lac@lobster.org).

- Review of AUP violation cases

The committee will review alleged violations of the LOBSTER Acceptable Use Policy brought to their attention, on a case-by-case basis. Clear violations of the policy may result in disciplinary actions, depending on the nature of the offence. If a participant does not conform to AUP's rules or to the recommendations of the committee, the use of the infrastructure will be prohibited to their institute.

- Handle conflicts

The AUP committee will also be responsible for handling conflicts that may arise between the LOBSTER' AUP and other national, European or company regulations. This kind of conflicts should be brought on the attention



**Acceptable Use Policy for the Fair Sharing and Use of the Infrastructure**      **IST-004336**

of the committee by all potential users of LOBSTER infrastructure and proper actions should be taken.

- Update the LOBSTER AUP document

The members of the committee will be responsible for suggesting and deploying any potential future changes in the AUP's rules, whenever needed. The committee will be in charge for informing all partners and current users of the infrastructure about the proposed changes. Finally, they will be responsible for updating the LOBSTER's AUP document and for disseminating it among all users.



## A1 LOBSTER Questionnaire – PART D

In this section you can find the questions concerning LOBSTER operation and policy, as they are including in LOBSTER' s questionnaire.

### Part D - LOBSTER operation and policy 4.0

Questions in this part concern your potential cooperation with the Lobster project as a pilot user. Brief description of the project is in attached document and also at <http://www.ist-lobster.org/>

#### 4.1: Cooperation with Lobster activities

Q: Please choose the appropriate response for each item:

- |  |           |
|--|-----------|
| • Intrusion attacks  | 1 2 3 4 5 |
| • Denial of service attacks  | 1 2 3 4 5 |
| • Viruses and worms  | 1 2 3 4 5 |
| • High-level traffic patterns (e.g. network overloads identifications) | 1 2 3 4 5 |
| • Low-level traffic patterns (e.g. TCP stack behavior in end host)     | 1 2 3 4 5 |
| • Traffic statistics   | 1 2 3 4 5 |
| • QoS measurement  | 1 2 3 4 5 |
| • Load/available bandwidth   | 1 2 3 4 5 |
| • One-way delay  | 1 2 3 4 5 |
| • Loss ratio   |           |

#### 4.2: Lobster service operation

Q: Who should operate the Lobster service in your network?

Please choose **only one** of the following:

- Your organization
- Independent consortium
- Other

#### 4.3: Expected output from Lobster system

Q: What kind of output from Lobster system do you prefer? Put also optional comments. Please choose all that apply and provide a comment:



- Raw data for own processing
- Processed data (e.g. warnings, alerts, graphs, tables)
- Aggregated data

#### **4.4: Data you could give to Lobster**

Q: What kinds of traffic data and information could you provide for (selected) Lobster participants? Put also optional comments. Please choose all that apply and provide a comment:

- Raw data (packet headers and payload)
- Filtered raw data
- Packet headers only
- Anonymized headers
- Statistics
- No data

#### **4.5: Required level of data anonymization**

Q: What kind of stored data anonymization would you require? Please choose **all** that apply:

- No anonymization
- Hashed payload preserving attacks signatures
- Removed payload
- Light sanitized IP address (unchanged network part of IP address)
- Removed payload + fully anonymized IP address
- Other:

#### **4.6: Issues of restricted participation in Lobster**

Q: Are there any organization, country or EU regulations that may restrict your participation in the Lobster project?

#### **4.7: Sensitive data that limit Lobster operation**

Q: Are there any kind of provided data/information that the Lobster project has to keep confidential?

#### **4.8: Acceptable usage of provided data**

Q: Is it acceptable to use your data for education or research? Put also optional comments. Please choose all that apply and provide a comment:

- Educational
- Research

#### **4.9: Bandwidth used by Lobster**



Q: Estimation of bandwidth (in Mb/s) that you could grant to operation of the Lobster system

**4.10: Solving Lobster installation/troubleshooting issues**

Q: Action you would take in case of installation or troubleshooting issues of the Lobster system. Please choose **only one** of the following:

- Deal with it yourself
- Grant remote access to other participant
- Other

**4.11: Solving Lobster system failure/malfunction**

Q: Support you would expect in case of Lobster system failure or malfunction. Please choose **only one** of the following:

- Cooperation with other participants
- Centralized Lobster help desk
- Other

**Lobster comments**

Q: Any other hints, comments or questions



## A2 Similar Infrastructures

- PlanetLab

[\[http://www.planet-lab.org/php/aup\]](http://www.planet-lab.org/php/aup)

- UK National Grid Service

[\[http://www.ngs.ac.uk/NGS-tacu.shtml\]](http://www.ngs.ac.uk/NGS-tacu.shtml)

- JANET

[\[http://www.ja.net/documents/use.html\]](http://www.ja.net/documents/use.html)

- NSFNET – vBNS

[\[http://www.nlanr.net/VBNS/vbns\\_aup.html\]](http://www.nlanr.net/VBNS/vbns_aup.html)