v. 2005

ACCEPTABLE USE POLICY

1. The hereby Acceptable Use Policy defines the rules applied to all the users of RENATER network[1].

2.

3. RENATER network is a network concealing risks of which the Signatory is informed and is fully responsible.

For its good use and security, it calls for a good cooperation among the different users. This cooperation is especially based on the Signatory's commitment on behalf of the sites'[2] users he is responsible for, directly or indirectly connected with RENATER network, to check over:

- the use of the network for **strictly professional purposes** according to the RENATER network objectives: education, scientific research, technical development, transfer of technologies, diffusion of scientific, technical & cultural information, new experimental services with a technically innovative aspect (see Appendix, 1 item 1) .

- a rational use of RENATER network resources in order to avoid any abuse of these resources, mainly by submitting to the GIP RENATER's prior agreement any implementation of applications causing a continuous traffic (see Appendix 1, item 2),

- a trusty use of RENATER network resources, by warning and abstaining from any improper use intended to disrupt or damage in any way the RENATER network (see Appendix 1, item 3);

---

1) RENATER network refers to the group of networks or communication nodes providing directly or indirectly, over the national territory, to authorized sites, with all or part of services for which GIP RENATER is the legal responsible, no matter who the operator or project manager may be.

2) The Signatory's Site(s) define(s) its different secondary sites (building, floors, premises) being under the Signatory's responsibility and connected directly or indirectly with the RENATER network.

- to transport and to give access to the network only for licit data, according to the appropriate legislation (see Appendix 1 item 4 : informative and not exhaustive list referring to French laws);

- not to give access, as a commercial or not, under payment or not, to the RENATER network to any non-authorized third party without GIP RENATER's prior and exact agreement (see Appendix 1, item 5);

- to implement technical and human resources in order to:
Γ ensure a permanent security level adapted to the state of art and the rules of this sector,

Γprevent any eventual acts of intrusion from or through his site(s) (see Appendix 2).
The nature of data transported or available on the network can determine, after proposal and under the responsibility of the Signatory, a particular security level which the Signatory will have to implement;

- more generally to comply with this present Acceptable Use Policy.

4. The Signatory of this A.U.P. is informed and expressly accepts that the GIP RENATER has the ability to control the correct use of the network (see Appendix 3). If the Signatory fails to meet his obligations as it is stated in the above clause 2, or after request of the administrative supervision authority of the concerned site(s), the GIP RENATER would interrupt the access to the RENATER network for these sites, at a national or international level.

5. The Signatory accepts that the GIP RENATER could take emergency measures, including the decision to limit or interrupt temporarily the access to the RENATER network of his site(s) at a regional, national, or international level, in order to preserve security in case of any troubling incident the GIP RENATER would be aware of.

However, these measures:

- will be taken respecting the best terms of time and after communication with the security responsible of the concerned site(s);

- will be applied only under the GIP RENATER's Managing Board approval procedure as well as under the condition of their technical and legal feasibility;

- and will be taken under the decision of security responsible persons, appointed by the founding members of the GIP RENATER.

In case the site(s) would suffer from repeated hostile actions from another site, and after the Signatory's or any concerned site(s)' request, the GIP RENATER would have to take restriction measures in the same terms and conditions as previously mentioned.

6. The Signatory is informed and expressly accepts that the GIP RENATER can modify this A.U.P., mainly in order to take into account legal evolution, which might occur in this sector; the Signatory will periodically receive notice of this update.

7. The Signatory of this A.U.P., representative of the moral personality of the site(s) (name, surname, title)

agrees to be fully acquainted with the A.U.P. of the "Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche" RENATER. He abides by these commitments, as well as all his users connected to the RENATER network belonging to the site(s) identified hereunder or to all the other sites which might be connected to the RENATER network, bound by a contract signed between the Signatory and the GIP RENATER.

Identification of the site or access sites ([3])
Address(es) :

The legal entity appoints as Security Responsible (Appendix 2)
Name, Surname:
Address:
Email address:
Telephone:
Fax number:

The Signatory:
Name, Surname:
Title:
Company:
Date:
Signature:
Stamp:

[3] The Site or the access sites mean(s) the one or those sites under the Signatory's responsibility, giving access to RENATER network for all the users served by the Signatory.
In the case of an entity with several sites having access to RENATER through the internal network of this entity, only the site entitled to have access to RENATER should be mentioned. However, RENATER A.U.P. is applied to all users of the sites connected to RENATER through this access. In the case one of the mentioned sites gave access to other entities, the GIP RENATER's agreement should be obtained first, in order for them to get lawfully access.

APPENDIX 1

1. The RENATER network used only for strictly professional purposes

The objective of the RENATER network is the transport of the traffic generated by activities related to education, research, technical developments, technology transfer, diffusion of scientific, technical and cultural information, new experimental services with a technically innovative aspect.

The activities related to the administration and management of the research, development or education centres are to be considered as research or education.

Further activities, mainly sale of services, will have to be justified by a prior written agreement by GIP RENATER, however, excluding from this condition sales activities related to education, research and technical development, as well as technological transfer and diffusion of scientific, technical and cultural information.

2. Rational use of RENATER network

In order for all users to meet a high quality level, the GIP RENATER limits the use of programs consuming the resources of the network (mainly for video diffusion). Under these conditions, the implementation of programs generating a permanent traffic is submitted to the GIP RENATER's a prior written agreement. Restrictions could be applied to time slots, or to the use of national or international connections heavily busy.

However, in order to permit the development and experimentation of these programs, the GIP RENATER will be in charge of the co-ordination of their deployment.

3. Trusty use of RENATER network

The Signatory has the responsibility to verify that no user on its Site(s) creates or generates on purpose data able to jam the connections of RENATER network or to deplete the equipment resources. Especially, automatons based on ICMP queries on the RENATER network routers are forbidden, except after GIP RENATER's prior written agreement.

4. Licit data transported on RENATER network

The transported and available network data issued by the users of RENATER network has to be licit. For this reason, the users have to respect all the legal dispositions, and especially the French legislation that follows:

- Intellectual Property Law which prevents the use, the reproduction and more generally to take advantage of protected works, mainly software, without the developer's or the rights owner's authorisation.

- The New Penal Code punishing violation of private life and minors' human dignity as well as technological crimes and offences.

- The law dated 29th of July 1881 punishing press offences, mainly slanders, denial acts, racism and insults.

- The law related to encryption.

An informative appendix of the actual French legal system is enclosed in this charter as appendix 4.

5. Supply of indirect access to RENATER network

An agreement procedure is applied to the Sites (see agreement form). The access to RENATER network is strictly reserved to authorized Sites. Consequently, every access whether commercial or not, under payment or not, to non-authorized party is forbidden without GIP RENATER's prior and written agreement. It is also forbidden to give access through the switched network or ISDN to people who are not users of these Site(s). The Signatory is the legal responsible in charge of the control of identification and access.

The notion of the indirect access refers to the retransmission or linked information services through the RENATER network as well.

The connection of other networks, national, foreign, international or sales service providers to the RENATER network, through an authorized site is submitted to the prior agreement of GIP RENATER. This connection will be subject to an agreement procedure.

Nevertheless, when a Site is part of a community or of a company (Industrial research centre within a company , school depending on a Chamber of Commerce, Education service and university research laboratory within an university hospital centre…), and its network is connected to networks belonging to this community or to this company, the Signatory :

- must not access to RENATER network to the users of this community or this company;

- has to inform the responsible person for these networks of the hereby A.U.P. terms, which refuse the access to RENATER for the users of those networks;

- has to take appropriate measures, so that these networks are isolated or screened, in case these ones are, directly or indirectly, the cause of problems on the RENATER network.

APPENDIX 2

Security

Being the only responsible for the equipment security, the Signatory commits himself to implement a security policy according to the state of art and the actual legislation.

For this reason, the Signatory should implement technical and personnel resources required in order to protect his Site(s) and to avoid aggressions towards other sites connected to the RENATER network or towards other networks or even towards the RENATER network from or through its (Site(s). Information on this matter is given on the Renater Web Site. The Signatory will particularly have to watch over the access to his Site(s) through the switched network or through the network ISDN.

However, the Signatory will have to appoint a person entitled "Security Responsible" and will make sure that users of his Sites get the relevant training and information.

The Security Responsible

Concerning events related to security, the Security Responsible should be given all the necessary operational powers to come up efficiently and in a short time in the case of a security problem, especially on request of the GIP RENATER, both at a connection level of the Signatory's authorized Site(s) and at level of a possible direct connections towards other sites.

When a security problem occurs on the Signatory's Site(s) involving one or more sites and/or the RENATER network, the security responsible of the affected site has to inform the GIP RENATER in the shortest time, and if necessary, to the best of his ability, to warn the other sites and participate to find a solution to the problem.

The obligation of information and instruction before all users

The Signatory has to inform the users of his Site(s), and especially the computer system managers, about the terms in the present A.U.P., in order to make sure they have been aware of its content as well as to ask the Directions of the other sites with access to the RENATER network through his own Site to process the same way. For that purpose, it is recommended to get a notice signed by the users indicating they are aware of the terms.

Besides, the Signatory commits himself to implement necessary instruction actions.

APPENDIX 3

The Signatory accepts that the GIP RENATER controls the good use of the RENATER network. For that purpose, he agrees with the fact that the GIP RENATER has access, especially before the concerned operators, to the administrative information of the network (such as volumetric data, problems, etc.) related to the Signer's Site(s). The GIP RENATER will consider this data as confidential, and only a global synthesis evaluation will be made public without the explicit agreement of the Signatory or his supervision authority.

Despite any contractual terms of confidentiality, the present A.U.P. has to be communicated to any moral entity or person using the RENATER network.

APPENDIX 4

Informative list of possible violations committed on the network

---

1. Violation stipulated by the New Penal Code

1.1. Crimes and offences against persons

- **Personality offences :**

- Violation of private life (art. 226-1 al.2, 226-2 al.2,art. 432-9 amended by Law 2004-669 of July,9,2004)
- Attack of personal image (art. 226-8)
- Slanderous accusations (art. 226-10)
- Violation of professional secrecy (art.226-13)
- Violation of the humans rights resulting from files and data processing (art. 226-16 to 226-24, issued from the computer and freedoms law of 6th of January 1978 amended)

- **Minors' human rights violation :** (art. 227-23; 227-24 and 227-28; concerning mainly pornographic messages likely to be seen by a minor age)
Law 2004-575 of June, 21,2004

1.2. Crimes and offences against property

- fraud (art. 313-1 and following)
- Automate data processing system damages (art. 323-1 to 323-7 relevant to the law dated 21st June 2004 related to computer) such as the access or the fraudulent staying in an automate data processing system, likely to damage or distort its functioning as well as to enter data fraudulently;

1.3. Cryptplogy

- Art. 132-79 (Law 2004-575 of June, 21,2004)

2. Press offences (law of 29th July 1881, amended)

- Incitement to crimes and offences (art. 23 and 24)
- Apologia for humanity crimes (art. 24)
- Terrorism (Incitement and apologia)
- Incitement to racial hate (art. 24)
- "Denial": unbelief of humanity crimes (art. 24 bis)
- Slanders (art. 31, 31 and 32)
- Insults (art. 33)

3. Violation of the Intellectual Property Code

- Illegal reproduction and use of an intellectual opus (including software) (art. 335-2 and 335-3 amended)
- Illegal reproduction and use of a design or a model (art. 521-4 amended)
- Illegal reproduction and use of a trademark (art.716-9 following amended)

4. Participation to the running of a gambling club ("cyber-casino")

- Art. 1 of the law of 12th July 1983, amended by the law of 16th December 1992.