REGULATION
FOR THE USE OF INFN INFORMATION TECHNOLOGY RESOURCES

JUNE 5th, 2016

1. General Principles

The National Institute for Nuclear Physics (INFN) is a research national public Institute governed by the provisions set forth in its statute.

INFN considers computing facilities, and network services, as well as related data and processed information, as an integral part of INFN assets and necessary to the achievement of its own institutional aims of scientific and technological research.

This regulation is meant to safeguard INFN information technology security system and to protect the privacy, integrity and availability of information and data produced, collected and anyway processed therefrom, including the personal ones.

INFN as partner of the association GARR Consortium – the Italian network of universities and research – and user of its related services and tools, in this regulation intends to ensure compliance with the rules dictated by the GARR Consortium.

INFN collects and processes data relating to the use of computing facilities and network services, only for specific, explicit and lawful purposes, in full accordance with the principles of need, relevance, correctness and non-redundancy. Consequently information systems and software are configured so as to minimize the use of personal and identification data.

Those who are entitled to use computing facilities and network services shall comply with the rules set forth hereinafter, which define and integrate the minimal obligations of behaviour laid down in the INFN code of conduct, in addition to behaviour inspired by principles of correctness and diligence.

2. Scope

This regulation applies to those who are entitled to use INFN computing facilities and network services.

3. Definitions

The terms **computing facilities** and **network services** refer to:

- computers and similar electronic devices, printers and other devices (e.g. scanner and storage systems) belonging to the Institute or anyhow connected to its network.
- equipment and networking infrastructure belonging to the Institute or anyhow connected to the Institute's network.
- local and geographical networking service with the exception of the geographical access guaranteed by agreements between Institutions and Federations (e.g. Eduroam)
- virtual machine instances or networking equipment;
- software and data purchased, produced or published by INFN.

In the framework of this regulation, computing facilities and network services considered as a whole can be defined as **information technology resources**.

Individuals using information technology resources belonging to INFN can be identified as:

- **User**: anyone who has access to INFN computing facilities and network services, according to the functions and professional duties they perform in the Institute.
- **User group contact person**: a person who coordinates the users and the usage of local computing resources belonging to one or more groups, experiments or services, in accordance with the guidelines provided by the Computing and Networking Service.
- **System administrator**: a professional who manages data processing system, even dealing with personal data, including database systems, local area networks and security equipment.
- **Computing and Networking Service**: the service responsible for managing central computing facilities, both internal and external networking of each structure, as well as implementing and developing them. It provides users with assistance in accessing the resources and the network and it has also expertise on the security of every computing facility in its own Structure.
- **Structure Director**: the person who shall ensure the scientific, organizational and administrative operation of each Structure as defined in the provisions set forth in INFN statute, in compliance with the guidelines adopted by the Board of Directors.

4. Access to IT resources

Upon identification and according to the rules laid down in this regulation, employees and associated personnel, as well as collaborators, guests, PhDs, specializing and graduating students, grantees and anyone else authorized, are allowed to access the INFN computing resources and network services.

Access authorization is granted by the Structure Director or by his delegate for a limited period of time, not exceeding the duration of their professional duties within INFN.

Access is personal, it cannot be shared or transferred and its use is only allowed in compliance with the rules of this regulation.

5. General provisions for the use of IT resources

Information technology resources, as essential to INFN, are made available for the achievement of INFN institutional objectives.

Users shall make use of IT resources safeguarding their integrity and ensuring the proper functioning.

Hence, the following activities are prohibited:

a) activities that contravene the national and international law, in breach of Community legislation or are not permitted by the ordinary usage of the networks and the services provided.
b) unauthorized commercial activities, or any other profit-making activities. The transmission of commercial and/or spamming advertising material, as well as the use of its resources by third parties for such activities.
c) activities liable to damage, destroy, jeopardize the security of INFN IT resources, or aimed at breaking the privacy and/or at damaging third parties, including the creation, transmission and preservation of images, data or any other material that is offensive,

obscene, defamatory, indecent or likely to undermine human dignity, especially when relevant to sex, race, religion, political opinions or personal and social condition.

d) activities in conflict with other institutional aims.

The use of IT resources for personal aims may be tolerated as long as it does not violate any applicable laws and complies with the rules of this regulation and with all the indications provided by INFN.

6. Specific provisions for the use of IT resources

In order to guarantee the security of computing facilities and networking services it is prohibited to:

1. connect computing facilities to the local network or to any services involving network connectivity without the authorization of the Computing and Networking Service;
2. wire, connect or modify network equipment without being authorized by the Computing and Networking Service;
3. use network addresses and names that have not been explicitly granted;
4. install hardware or software systems that enable access to IT resources without being authorized by the Computing and Networking Service;
5. provide access to IT resources to persons who have not been explicitly authorized;
6. disclose information on IT resources structure and configuration, especially those concerning remote access;
7. access the Computing and Networking Service areas, as well as the areas reserved for network equipment, without being authorized;
8. undertake any other action aimed at degrading system resources, preventing authorized access to resources, getting greater resources than those authorized or accessing resources by violating the security measures.

Moreover **users** shall**:**

1. act in compliance with the law and in accordance with the security directions provided by Computing and Networking Service. They are required to ensure the privacy of processed personal data by proper observance of the rules established by INFN, which are available at the following web page: www.infn.it/privacy/;
2. take into account the guidelines provided by the Computing and Networking Service concerning the selection of computing devices to use, especially if they concern security-related features. They shall prefer systems and procedures that offer the highest levels of protection;
3. be responsible for the data and for the software they install on the computers entrusted to them: they are required to examine software carefully and in advance and do not install any software with no regular licenses.
4. protect from unauthorized access data used and/or stored in the computers and systems they are allowed to access;
5. carefully evaluate the reliability of external services, including *cloud* services, in terms of security, storage and data confidentiality.
6. follow the Computing and Networking Service recommendations concerning the regular back up of data and used programmes;
7. protect their account avoiding to choose obvious passwords and in the event of multiple authentication systems by using different passwords for each system.

8. not share their passwords, nor allow even occasional use by anyone other than the account holder;
9. immediately notify any incidents, suspected abuses and security breaches to their contact person and to the Computing and Networking Service.
10. use updated anti-virus software where operating systems require that. They shall take care to scan all software and files exchanged over the network and all removable media they use;
11. not maintain unused remote connections nor leave their work station unattended with unprotected open connections.

7. Tasks of the user group contact person

The **user group contact person**:

1. delivers to his group any Computing and Networking Service directions concerning the security of resources and their proper use.
2. when needed, provides Computing and Networking Service with information or access to the computing facilities of his group.

8. Tasks of System administrators

System administrators, in addition to abiding by all the above-mentioned rules, shall

1. keep systems at the appropriate level of security for their use;
2. verify regularly system integrity;
3. check and maintain system logs for the time necessary to test the preservation of security standards;
4. notify immediately incidents, suspected abuses and security breaches to the Computing and Networking Service, and collaborate to handle them;
5. install and keep anti-virus software up-to-date, for operating systems that require it;
6. not inspect personal data and correspondence they become aware of and consider them as strictly confidential. They shall not report, duplicate nor transfer content and information on their existence to unauthorized persons;
7. in case of servicing or maintenance work on the systems they manage, they shall prevent as far as possible access to information and to personal data stored in the systems;
8. attend training courses in technical-managerial matters and network security, as well as in data protection and correspondence confidentiality.

9. Tasks of the Computing and Networking Service

In order to keep the highest level of security in the local networks and in relation with the technological development of its branch, the Computing and Networking Service shall:

1. verify that remote logins to the local facilities take place exclusively through the use of protocols providing authentication and encryption of the transmitted data;
2. limit the internal use of services and software sending unencrypted passwords;

3. disable non-essential services on the equipment under its jurisdiction and restrict the number of privileged users to the minimum strictly needed for performing activities of coordination, control and monitoring of the network and its related services;
4. perform account review on a yearly basis;
5. monitor managed systems by recording privileged accesses, possible changes to system files and any unauthorized use of network services;
6. implement filtering and logging systems on the perimetric network devices.
7. help to preserve and increase the security of resources entrusted to users.

10. Provisions for the use of external services

The INFN may use external services, including the *cloud*, in processing personal data - whether common or sensitive - or data of particular importance for the Institute, only after checking out the risks and benefits related to the offered services, the limits on circulation and data transfer, as well as the reliability of the supplier, the existence of guarantees and precautions for storage, persistence and data confidentiality, in addition to data processing liability.

11. Processing data obtained by using computing facilities and by accessing the network

The remote control of users and related data processing achieved by installing specific hardware equipment or software, is prohibited by INFN, in compliance with the principles of freedom and dignity. In particular:

a) systematic recording and reading of e-mail messages, beyond what is necessary to carry out the e-mail service;
b) systematic reproducing and recording of web pages viewed by the user;
c) reading and registering characters entered by keyboard or similar devices;
d) unauthorized inspection of laptops entrusted to the user.

Regarding the network access, the Computing and Networking Service matches information on the address, the computer name and its user for the purposes mentioned below; it does not record the content of connections, however it may collect some information concerning the transactions occurred such as: hub connections, start and end of timestamps of transaction and amount of data transferred.

The data referred to in the previous paragraph shall be retained for a period not exceeding one year and can be used by the Computing and Networking Service staff only for security purposes and for systems optimization.

The Structures, where proxy server or other session control systems are installed, may save the log files containing information on web pages – whether internal or external - that are accessed from local computers. The Computing and Networking Service saves such information for a period not exceeding seven days; it analyses and processes it only if necessary to guarantee the security of the system and its proper operation.

12. Data collection relating to email service

The Computing and Networking Service records email messages' date, time, sender and recipient's addresses, as well as the result of antivirus and anti-spam software analysis, conducted for the needs related to the operation, security and integrity of email service.

The data recorded, which are also used for statistics, are stored for a period not exceeding one year and can be accessed only by the personnel specifically in charge of the Computing and Networking Service.

For the same purposes, Structures that back up email messages, shall keep the back up copies for a period not exceeding one year. The Computing and Networking Service is responsible for taking care of the backup.

Where compatible with its organization, each Structure can provide shared email addresses through distribution lists, as well as auto-reply messages in case of a programmed absence of the list managers.

A user's mailbox is disabled within two months following the expiry date of the period in which the user was granted access. Within this period the user is obliged to transfer any useful communications and other communications occurred meanwhile to the Director or a delegate of theirs. In any case the mailbox content is deleted one year after the end of the access grant.

Extending the periods referred to in this paragraph is at the Director's discretion, when deemed necessary.

In the event of the mailbox owner's inability or hindrance, the Director, or a delegate of theirs, may have access to the mailbox for a period not exceeding one month from the date when they became aware of the situation that caused such inability or hindrance.

13. Further measures for protecting information systems

In order to ensure the operation, availability, optimization, security and integrity of information systems and prevent inappropriate uses, INFN adopts measures that allow to check abnormal behaviours or conducts which this regulation does not cover, in accordance to the above mentioned necessity, relevance, and non-redundancy principles. The Computing and Networking Service can process recorded data for the purpose of pointing out anomalies in the network traffic or conducts not permitted by this regulation.

In the event of detected damages or upon the occurrence of behaviours which are abnormal and not permitted despite the adoption of precautionary technical measures, the Computing and Networking Service, unless in cases of emergency, shall inform the parties concerned and carry out any further investigations to put into effect the necessary measures aimed at stopping any harmful and unauthorized conducts.

In case of recurrence of prohibited behaviours, already reported or particularly serious, the Computing and Networking Service manager shall adopt all the technical measures needed, informing immediately the Structure Director who shall take further actions pursuant to the following point.

The Structure Directors are responsible of personal data processing. They shall take any necessary actions to ensure that the persons entitled to process data relating to the use of internet and email perform only operations strictly necessary in pursuit of their aim and do not carry out remote control activities, not even on their own-initiative.

14. Policy violation

Any infringement of the present Regulation will result in the suspension of access to computing facilities, without prejudice to any disciplinary, civil or criminal proceedings.

15. Note

This regulation provides information pursuant to Article 13 of legislative decree 30 June 2003, no.196 and Article 4, paragraph 3, of the law 20 May 1970 no. 300 and followings concerning the terms and purposes of processing personal data related to the use of computing facilities and network services.
INFN ensures that this regulation and its subsequent updates have the widest dissemination among users through its publication on the web pages of each structure, as well as by delivering it to everybody in electronic or printed mode, in any mode suitable to prove it has been delivered.

This Regulation repeals and replaces in its entirety all the previous regulations adopted on this subject.

16. Review Clause

This regulation is periodically updated according to the technological evolution and the regulations existing in this branch.