



**ISTITUTO
ITALIANO DI
TECNOLOGIA**

ICT Policy

Revision	Description of Modification	Author	Approval	Date
04	Art. 1.1	ICT	E.C.	11/05/2009
05	Art. 1.1	ICT	E.C.	21/10/2015
06	Complete revision	ICT	E.C.	25/09/2017

SUMMARY

1. Objectives and goals	3
2. Overview and definitions	3
2.1 Overview	3
2.2 Definitions	3
3. Execution	4
3.1 Protection of workers and rights to the protection of personal data	4
3.2 Use of Information Technology Systems	4
3.3 Handling and protection of data	5
3.4 Information technology security	5
3.5 Control activities	6
3.6 Responsibility	6

1. Objectives and goals

- The present Policy refers to all the information technology and telecommunication systems and equipment owned by or available to the IIT Foundation (hereafter also referred to as "Information Technology Systems").
- The present Policy is aimed at anyone who is an employee or a collaborator of the IIT Foundation or who is an employee of a partner of the IIT Foundation and who carries out scientific research, professional activities or study within the IIT structure. The aforementioned categories will hereafter also be referred to as "Users".
- The aim of the present Policy is to establish the correct usage of Information Technology Systems within the IIT Foundation (hereafter also referred to as "Foundation" or "IIT"). The following rules are aimed at protecting IIT and the Users from the risk of the Information Technology Systems being compromised, via the undue transmission of personal and confidential data, and the relative legal consequences, as well as at rendering the use of Information Technology Systems more efficient.

The following dispositions will also make reference to a number of definitions provided for by regulations in force regarding the protection of personal data.

2. Overview and definitions

2.1 Overview

The Foundation adopts instruments, processes and procedures that are aimed at guaranteeing the security of information technology and encouraging the assumption of responsibility by individual Users.

The Information Technology Systems made available to Foundation Users are one of the strengths of the Foundation but, at the same time, they can also constitute sources of risk in terms of the security of information handled and the image of the Foundation. For this reason, the use of the aforementioned Information Technology Systems must always be characterised by diligence and correctness.

The prescriptions contained in the present Policy are in addition to the specific instructions already provided to all Users, also in execution of the Code of Behaviour and Scientific Conduct.

2.2 Definitions

Name	Abbreviation	Description
User	UT	Anyone who is an employee or a collaborator of the IIT Foundation or who is an employee of a partner of the IIT Foundation and who carries out scientific research, professional activities or study within the IIT structure.
Information Technology Systems	S.I.	Information technology and telecommunication systems and equipment owned by or available to the IIT Foundation.
Telecommunication Network	R.T.	The collection of devices and their connections (either physical or logical) which allow for the transmission and reception of information of all types between two or more users situated in geographically distinct positions, which carry out the transfer of data via cable, radio or other electromagnetic or

Name	Abbreviation	Description
System Administrator	A.S.	optical systems. A professional figure responsible for the management and maintenance of a computing system or its components. In the information technology sector this also refers to other figures which are equivalent from a point of view of risks relative to the protection of data, such as database administrators, network and security apparatus administrators and administrators of complex software systems.
Data Controller	T.T.	The physical person, legal entity, public administration or any other body, association or organism responsible, also together with other controllers, for decisions regarding the objectives and methods of data handling and instruments used, including security profiles.
Personal Data	D.P.	Any information relative to physical persons who may be either directly or indirectly identified or identifiable through reference to any other information, including a personal identification number.

3. Execution

3.1 Protection of workers and rights to the protection of personal data

The IIT Foundation, in its role as data controller, carries out the handling of personal data in full respect of regulations in force that are applicable with regards to the protection of personal data and the observance of the principles of necessity, correctness, pertinence and non-excessiveness, solely for determined, explicit and legitimate purposes and in the least invasive measure possible.

Without prejudice to the above, System Administrators may monitor instruments, systems, network traffic and the use of resources in general at any moment, including on a periodical basis, in order to provide for the correct maintenance of systems and to guarantee safety.

3.2 Use of Information Technology Systems

1. The use of Information Technology Systems provided to individual Users must be for professional objectives. As a partial exception to this principle, limited to personal devices, the IIT Foundation allows moderate and reasonable private use. Said use must be limited and governed by criteria of common sense, and must not in any way compromise or obstruct professional use. The use of Information Technology Systems for "private" purposes is allowed exclusively for the storage of data files, photographs or films, and said activity must therefore be clearly identified and limited and must not hinder or limit professional use.
2. Shared work areas are strictly for the storage of professional information and must not in any way be used for other purposes. Therefore, any files which are not related to professional activities must not, even for short periods, be stored in said areas, which are subject to activities of administration and control by System Administrators (a list of Administrators can be consulted on the Foundation's Intranet).
3. The email address provided by the Foundation is exclusively for professional use.
4. Access to IIT networks via personal Information Technology Systems may take place under the condition that this is carried out in full respect of the provisions of the present Policy.
5. The use of Information Technology Systems is subject to restrictions deriving from regulations in force and dispositions in the present policy. In particular, it is forbidden to use Information Technology Systems and Telecommunication networks:

- i. in ways that do not conform to criminal, civil and administrative regulations;
- ii. for purposes that are incompatible with the objectives and institutional activity of IIT;
- iii. to allow unauthorised access to network resources either internal or external to IIT;
- iv. for activities that violate the confidentiality of other Users or third parties;
- v. for activities that negatively influence normal operativeness or which compromise usability and performance;
- vi. for activities that provoke the unauthorised transfer of information;
- vii. for activities that violate regulations for the protection of original work;
- viii. in ways that do not conform to the *Acceptable use policy* of the GARR network (available on the Foundation's Intranet).

For details relative to the use of Information Technology Systems, please consult the relative operational procedures published on the Foundation's Intranet.

3.3 Handling and protection of data

Data and documentation that are important to the Foundation, including, for example, classified data (protocols, personal data) and/or confidential data, and data relative to the Foundation's Intellectual property, are held on Information Technology Systems that have been surveyed and approved by the Foundation, which has previously verified that the technical and contractual aspects respect applicable regulations in force as well as guidelines regarding the protection of personal data and the management of Information Technology Systems.


In the case of sudden or prolonged absence during which working necessities must be addressed without being postponed or could be detrimental to the IIT, the Foundation reserves the right to access the professional content of Users, except content as stated in 3.2.1., following a specific procedure and in accordance with the Italian Data Protection Authority's Guidance and the principles stated at paragraph 3.1.

Users who store data and/or documentation belonging to the Foundation on Information Technology Systems that have not been previously surveyed and approved by the Foundation are responsible for the same and for any damages to the Foundation and/or third parties caused by their loss or theft.

3.4 Information technology security

All Users are required to actively collaborate with the Foundation in order to reduce to a minimum the risk of attacks on Information Technology Systems that may compromise services or cause the loss of data and/or documentation that is important to IIT through malicious software (for example worms, viruses, Trojan horses, etc.) and, more generally, through the actions of programmes as specified in article 615-quinquies of the Penal Code. All users are therefore required to:

- connect to the Foundation's network exclusively with Information Technology Systems with functioning and updated antivirus software installed;
- verify all external devices before opening any files;
- pay the utmost attention to the contents of suspicious or unexpected emails;
- perform regular backups and, if possible, use encrypting techniques to protect data held outside Information Technology Systems that have been documented and approved by the Foundation;

 ISTITUTO ITALIANO DI TECNOLOGIA	Policy ICT	P_11
----------------------------------------------------------------------------------------------------------------------------------	------------	------

- promptly inform the ICT Management of threats that the antivirus software is unable to automatically eliminate

3.5 Control activities

System Administrators are authorised by the Foundation to carry out forms of non-individual control on the network and all devices which form part of the same.

In order to provide for the correct maintenance of systems and guarantee security, System Administrators may monitor instruments, systems, network traffic and in general the use of resources at any time, even on a periodical basis, paying the utmost attention to the safeguarding of User privacy. In no case will covert targeted checks be carried out. Initial controls, with reference to operations considered dangerous or which are in any case unauthorised, will be carried out exclusively on all Users in general. The continuation of unauthorised activity will authorise the Foundation to carry out more in-depth investigations, carrying out checks on more focused groups. In the event that further abuse and/or behaviour which threatens the security of Information Technology Systems, and/or which is damaging to company property, and/or which constitutes a crime, is registered, activities of control will be carried out on a personal level.

The Foundation reserves the right in any case to report any unauthorised behaviour of which it is aware to the Judicial Authorities.

System Administrators may at any time proceed with the prompt removal of all files or applications which are considered to be a threat to security both from work stations and network units.

3.6 Responsibility

Those failing to respect the present policy may be subject to immediate suspension of access privileges to Information Technology Systems by the IIT Foundation, which reserves the right to execute disciplinary procedures.

Furthermore, the violation of regulations regarding safety in the management and use of Information Technology Systems and the protection of personal data can lead to further and independent consequences of a civil, criminal and administrative nature.