



**ISTITUTO  
ITALIANO DI  
TECNOLOGIA**

<b>Information Security Policy</b>
------------------------------------

Review	Change description	Author	Approval	Date
01	First publication	ICTD	EXECUTIVE COMMITTEE	22/03/2019

## TABLE OF CONTENTS

1. Objectives and purpose .....	3
2. Premise and definitions.....	3
2.1 Premise .....	3
2.2 Definitions .....	3
3. Key operators and responsibilities .....	4
4. Documents and tools .....	5
5. Implementation .....	7
5.1 Information classification .....	7
5.2 Data management and protection .....	8
5.3 Responsibilities .....	9
6. Compliance and exceptions.....	9
6.1 Compliance assessment.....	9
6.2 Exceptions .....	9

## 1. Objectives and purpose

- The object of this Policy is information security, whether such information be stored, in transit or in use, managed via all systems and ICT equipment that belongs or is available to the IIT Foundation (hereinafter referred to as “ICT Systems”).
- This Policy is addressed to whomever is in a relationship of non-directive employment, of directive employment, of coordinated and continuous collaboration with the IIT Foundation, along with its external personnel, which carries out scientific research, professional or study activities within the IIT buildings. The above-mentioned categories of subjects will be referred to hereinafter as “Users”.
- Included among those to whom this Policy is addressed are also all third parties, such as suppliers and research bodies, which manage IIT Foundation information via ICT systems and equipment. These categories of subjects will be referred to hereinafter as “Third Parties”.
- The purpose of this Policy is to establish the rules for classifying and securing information via the ICT systems used by the IIT Foundation (hereinafter also referred to as “Foundation” or “IIT”).

In the following rules reference will also be made to the current rules and regulations that are applicable with regards to personal data protection.

## 2. Premise and definitions


### 2.1 Premise

The Foundation adopts tools, processes and procedures that are useful in view of ensuring information security and encouraging the individual Users responsibility and awareness.

The ICT systems made available to Foundation Users constitute one of its strong points, however, such systems have the potential of becoming a source of security risk for the information treated and for the Foundation's image. For this reason, it is necessary to assess the security risks in managing information, beginning with their classification. The information classification allows for both their informed management on behalf of Users and for the implementation of the necessary technological and procedural security measures to mitigate such risks.

### 2.2 Definitions


Name	Abbreviation	Description
User	US	Whoever is in a relationship of employment or collaboration or is external personnel affiliated with the IIT Foundation, who carries out scientific research, professional or study activities within IIT buildings.
ICT System	ICT S.	The ICT systems and equipment belonging or available to the IIT Foundation.
Communication Network	C.N.	All devices and connections (physical or logical) which allow for the transmission and reception of information of any kind between two or more users located in geographically distinct places, transferring such information via cables, radio systems or other electromagnetic or optical systems.

 <b>ISTITUTO ITALIANO DI TECNOLOGIA</b>	<b>Information Security Policy</b>	<b>P 26</b>
--	------------------------------------	-------------

<b>Name</b>	<b>Abbreviation</b>	<b>Description</b>
Personal Data	P.D.	Any form of information that concerns an identified or identifiable physical person («concerned individual»); a physical person is to be considered identifiable when they can be identified, directly or indirectly, with a particular reference to an identifying aspect such a name, identification number, residency information, an online identification code or one or more characterising elements of their physical, physiological, genetic, psychological, economic, cultural or social identity.
Special Personal Data	S.P.P.	Personal data that reveals the racial or ethnic origin, political opinions, religious or philosophical convictions, or trade union membership, but also genetic data, biometric data that can unequivocally identify an individual, data regarding health or sex life or the sexual orientation of a person.
Integrity		The safeguarding of accuracy and completeness of information.
Availability		Information must be accessible to an authorised body who requests it.
Authenticity		The origin of the information can be verified.
Non-repudiation		The origin and content of the information are demonstrated and certified.
Confidentiality, Integrity and Availability	CIA	Security characteristics in view of protecting information and ICT System
Risk		The possibility of suffering damages connected to circumstances that are more or less predictable.
Endpoint		Any laptop/desktop computer or mobile device
Server		A host which provides internet access
Application		Software functioning on a remotely accessible server
SaaS		An application software distribution model whereby a software producer develops, operates (directly or via third parties) and manages a web application that they make available to their clients via the internet

### 3. Key operators and responsibilities


<b>Operator</b>	<b>Abbreviation</b>	<b>Key responsibilities</b>
ICT Directorate	ICT	The development and management of the internal network are assigned to the ICT office which operates in line with the Foundation's institutional organs' deliberations and in close collaboration with GARR.
GARR	GARR	Is the ultra-broadband network dedicated to the Italian research and education community. Its main objective is to provide high-performance connectivity and to develop innovative services for the daily activities of researchers, professors and students as well as for international collaboration.
User	US	<p>All users who in any way interact with the Foundation's data via ICT tools accept this Policy without reservations.</p> <p>The Users who manage and preserve data and/or documents of the Foundation on ICT Systems, that are not previously checked and approved by the Foundation, are responsible for the classification of the level of information security risks and for the implementation of the security measures necessary for mitigating such risks.</p>

 <b>ISTITUTO ITALIANO DI TECNOLOGIA</b>	<b>Information Security Policy</b>	<b>P 26</b>
--	------------------------------------	-------------

<b>Operator</b>	<b>Abbreviation</b>	<b>Key responsibilities</b>
Director	Director	The Directors of the central administration structures are responsible for the classification of the level of information security risks for information managed by their own department and for identifying the ICT S. that manage such information.
Principal Investigator	P.I.	Every P.I. is responsible for the classification of the level of information security risks for information managed by their own area and for identifying the ICT S. that manage such information.
ICT Contact		The technical figure who is responsible for managing the ICT systems that are not managed by the ICT Directorate directly.

## 4. Documents and tools

<b>Type</b>	<b>Name</b>	<b>Use</b>	<b>Link</b>
Policy	ICT Policy	Establishes the correct use of ICT systems in the IIT Foundation (hereinafter also referred to as “Foundation” or “IIT”), protecting IIT and its Users from the risk of compromised ICT systems, from the illicit distribution of personal and private data and from the relative legal consequences, while also making the use of the ICT systems more effective.	<a href="https://short.iit.it/ictpolicy">https://short.iit.it/ictpolicy</a>
Document	Examples of information risk classification	Lists assessment examples of information security risks.  This appendix, given its nature, is updated in line with the ICT Directorate's needs; its updates do not require the approval of the Executive Committee.	<a href="https://short.iit.it/risk-classification">https://short.iit.it/risk-classification</a>
Document	Information security measures	Lists the security measures to be implemented based on the information security risk classification regarding the information on the Foundation's ICT system.  This appendix, given its nature, is updated in line with the ICT Directorate's needs; its updates do not require the approval of the Executive Committee.	<a href="https://short.iit.it/information-security-measures">https://short.iit.it/information-security-measures</a>
Document	Approved ICT systems by level of information security risk	Lists the Foundation's ICT systems and the level of information security risk for which its use has been approved.  This appendix, given its nature, is updated in line with the ICT Directorate's needs; its updates do not require the approval of the Executive Committee.	<a href="https://short.iit.it/approved-services">https://short.iit.it/approved-services</a>

 <b>ISTITUTO ITALIANO DI TECNOLOGIA</b>	<b>Information Security Policy</b>	<b>P 26</b>
--	------------------------------------	-------------

<b>Type</b>	<b>Name</b>	<b>Use</b>	<b>Link</b>
Form	Security Risk Exception	Form for managing policy exceptions.  This appendix, given its nature, is updated in line with the ICT Directorate's needs; its updates do not require the approval of the Executive Committee.	<a href="https://short.iit.it/risk-exception">https://short.iit.it/risk-exception</a>

## 5. Implementation

### 5.1 Information classification

To protect the information managed by the ICT, both stored and in transit or use, and in order to implement adequate security measures, the information is classified into three levels of risk (High, Medium, Low) in relation to the protection of Confidentiality, Integrity and Availability (hereinafter referred to as CIA). The three levels of risk are defined as follows:

#### 1. High Risk

The information and systems<sup>1</sup> are of a High level of risk if at least one of the following conditions is true:

- the loss of Confidentiality, Integrity or Availability of the information can have a significant adverse impact on Intellectual Property or on the mission or reputation of the Foundation, or a significant economic or legal impact
- the protection of the information is required by Law<sup>2</sup>
- the protection of the information is required by contracts or certifications of national or international standards (such as the ISO standards)

#### 2. Medium Risk

The information and systems are of a Medium level of risk if:

- they are not of a High level of risk
- the information or ICT services are not typically addressed to the public or external bodies
- the loss of Confidentiality, Integrity or Availability of the information can have a midly adverse impact on the Intellectual Property or on the mission or reputation of the Foundation, or a limited economic or legal impact.


#### 3. Low Risk

The information and systems are of a Low level of risk if:

- they are not of a High or Medium level of risk
- the information or ICT services are typically addressed to the public or external bodies
- the loss of Confidentiality, Integrity or Availability of the information would not have a significant impact on the Intellectual Property or on the mission or reputation of the Foundation, nor would it have a significant economic or legal impact.

<sup>1</sup>The level of risk for an ICT system is determined by the highest level of risk of the information it manages.

<sup>2</sup> Particularly worthy of consideration are the requirements of the current rules and regulations with regards to the protection of personal data.

 <b>ISTITUTO ITALIANO DI TECNOLOGIA</b>	<b>Information Security Policy</b>	<b>P 26</b>
--	------------------------------------	-------------

For information containing Personal Data in accordance with the European and national rules and regulations with regards to the protection of personal data, it is always necessary to define the time limit for data conservation.

Every Director and every P.I. is responsible for the classification of the information managed by their own department and is obliged to notify their staff of the outcome of such classifications and to maintain them within their own storage.

The users who manage and conserve data and/or documents on Foundation ICT Systems must respect the requirements of this Policy.

The document “Examples of information risk classification” contains a number of classification examples with regards to information.

The document “Approved ICT systems by level of information risk” contains a list of Foundation ICT systems and the level of risk for which its use is approved.

The information is also classified as information either containing or not containing Personal Data. The presence of Personal Data requires an evaluation of the relative risks with regards to the protection of personal data in accordance with the current rules and regulations and with the Policies and procedures adopted by the Foundation.

## **5.2 Data management and protection**

The information and documents will be managed and preserved on ICT Systems that are registered and approved by the Foundation which has pre-emptively verified that the technical and contractual elements respect the current applicable rules and regulations and the guidelines referring to the protection of personal data and ICT Systems management.

The appropriate security measures are applied to every ICT System, aimed at minimising risks for the Confidentiality, Integrity and Availability of information both stored and in transit or use. The security measures adopted must be in line with the level of risk that has been identified (High, Medium, Low) in accordance with the content of section 5.1.

When each ICT System is due to be disposed of, all data and information contained therein must be permanently removed.

The document “Information security measures” lists the security measures to be adopted by every ICT S. in relation to the identified level of risk.


Along with the security measures, for each ICT S. the ICT Directorate, where necessary, identifies and applies further specific security measures in relation to the type of information managed and the relative risks, to the way in which the ICT S. are managed and to the applicative and infrastructural context.

Specific security measures must be adopted to protect information managed via mobile devices such as smartphones, tablets, laptop computers and other similar means, to mitigate risks in the case of theft or loss of such devices.

Should one wish to manage and preserve data and/or documents on other ICT systems that have not been pre-emptively registered and approved by the Foundation, the following must be verified:

- that the security measures, as listed in the document “Information security measures” relating to the identified level of risk, are implemented



 <b>ISTITUTO ITALIANO DI TECNOLOGIA</b>	<b>Information Security Policy</b>	<b>P 26</b>
--	------------------------------------	-------------

- that any further specific security measures deemed appropriate are implemented.

Nonetheless, users who manage and preserve data and/or documents on ICT Systems that are not pre-emptively registered and approved by the Foundation remain responsible for any damages to the Foundation and/or third parties caused by their loss, theft, modification, unauthorised access or data distribution.

### **5.3 Responsibilities**

Should a User violate the rules stated in this policy, they are liable to be immediately suspended from accessing the ICT Systems by the IIT Foundation.

To all personell may be applied, along with the Code of Behaviour and Scientific Conduct and the Organisational Model in accordance with Law 231/2001

Moreover:

- with regards to employed non-executive personnel, the IIT disciplinary regulation may be applied;
- with regards to employed executive the disciplinary regulation for executive may be applied, if required;
- for coordinated and continuous collaborators the Foundation may enact an early termination as determined by the coordinated and continuous collaboration contract stipulated between the parties;
- for personnel who are affiliated, the procedures specified in the affiliation agreement and/or agreement between the parties with regards to violating the Policy and procedures of the host institution may be applied.

Every User who manages and preserves Foundation data is responsible to guarantee that this policy is respected by all third parties who are to intervene on the treatment of said data.

In the case of third parties, violating the policy may be sanctioned based on specific contractual clauses which allow, in the gravest of cases, for the termination of the contract in accordance with the requirements listed in art. 1456 of the Italian Civil Code.

Furthermore, the violation of rules and regulations regarding security during the management and use of ICT Systems and the rules regarding the protection of personal data may also incur further and autonomous consequences of a civil, penal and administrative nature.

## **6. Compliance and exceptions**

### **6.1 Compliance assessment**

The ICT Directorate is authorised by the Foundation to evaluate the accuracy of the levels of risk assigned to information in the ICT S. and to assess the security measures put in place to mitigate such risks (see the “ICT Policy”).

### **6.2 Exceptions**

Any exception to this policy must be approved beforehand by the ICT Directorate. To request an exception, one must use the “Security Risk Exception” form.