ISTITUTO
ITALIANO DI
TECNOLOGIA

Access procedure to data in case of sudden or extended absence

Revision	Description of change	Author	Approval	Date
01	First issue	ICTD	SD DG	21/12/2018

Table of Content

1. Objectives and purposes

The objective of this procedure is to define and regulate, in accordance with the ICT Policy of the Italian Institute of Technology Foundation (hereinafter, also "Foundation" or "IIT"), the methods of access to company data managed by users (hereinafter: "Users") available in the Information Systems of the Foundation, such as, for example, the Foundation's e-mail service, PCs, shared directories or cloud services provided by the Foundation, in cases of sudden or extended absence of the User, during which there are urgent needs related to work or activities from which may arise detrimental outcomes for the Foundation. This procedure (hereinafter, for the sake of brevity, also "Emergency access procedure to data") ensures the full transparency of the Foundation work and protects Users from access that may be aimed to achieve different and further objectives, with particular reference to confidentiality of the Users, in compliance with the legislation on worker protection. Users are made aware of this procedure and must take them into account when using IT systems.

This procedure is not related to any access made for in-depth analysis activities or checks carried out by the Foundation in case of possible misconduct, of any nature, that could have been carried out against it or third parties, even in violation of internal regulations.

2. Introduction and Definitions

a. Introduction

As part of the activities carried out for the Foundation, Users of Information Systems may temporarily have available, in their data spaces (e.g. e-mail, PCs, directories or cloud services), company information not available elsewhere, that can be necessary to undertake the Foundation activities during a period in which the Users are not able to provide them, in particular in case of sudden or extended absence. In these cases, while respecting the rights of the Users, the Foundation reserves the right to access the resources entrusted to the Users in order to retrieve the above information. This access may be necessary to verify the pending activities of Users that, if not carried out, may result in detrimental outcomes for the Foundation. In any case, before the activation to the Emergency access procedure, the Foundation will try to contact the Users, in due time and in a manner compatible with the operational needs, to notify the latter of the intention to activate this procedure, in order to allow them, where possible, to personally provide the necessary data.

b. Main definitions

Name	Abbreviation	Description
Personal Information	P.D.	Any information related to a natural person, identified or that can be identified, even indirectly, by reference to any other information, including a personal identification number.
IT systems	I.S.	The IT and telecommunication systems and equipment owned by, or available to the IIT Foundation
Minutes of emergency access to data	Minutes	Tracking useful information related to access to emergency data
Policy	ICT Policy	Define the correct use of IT systems in the IIT Foundation by protecting IIT and Users from the risk to compromise IT systems, from the undue disclosure of personal and/or confidential data, and the related legal consequences, furthermore, it makes the use of IT systems more effective.

3. Main players and responsibilities

Actor	Abbreviation	Greater responsibility
ICT Directorate	ICT	The development and management of the internal network is entrusted to the ICT Directorate, which works in accordance with the resolutions of the institutional bodies of the Foundation and in close collaboration with GARR.
User	User	Anyone who has an employment or collaboration relationship with the Foundation and external staff, affiliated to the IIT Foundation, that carries out professional,study or scientific research within IIT structuresUsers of the Foundation's network, in particular, are persons who belong to all the research and service structures directly connected to the Foundation's internal network. All Users who, for any reason, use the Foundation's network fully accept this procedure.
System Administrator	SA	Professional position for management and maintenance of a processing system or its components. In the IT environment, there are other profiles that are similar in terms of data protection risks, such as database administrators, network and security administrators and administrators of complex software systems. The System Administrator, pursuant to the Provision of the Protection Authority for Personal Data Processing, of 27 November 2008, is selected on the basis of experience, skills and reliability.
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.

4. Procedure: description

The Emergency access to data procedure is activated by the Scientific Director when s/he becomes aware, also upon notification by other staff members of the Foundation, of the need to access company data managed by an absent User that cannot provide independently the data. S/he can then, at any time, entrust the continuation of the activities to his/her representatives. The person who carries out these activities, whether s/he is the Scientific Director or his/her representative, hereinafter is the "Access Manager".

The Access Manager, before going on with the Emergency access to data procedure, evaluates:

- the real need to access data without waiting for the return of the User, in terms of potential impacts on the Foundation's activities and complexity in obtaining the data through another method, in particular the impacts that the unavailability of data could have on the activity of the Foundation, and compares these two solutions with the impacts, even if limited, that access to the data areas of the User could have on the privacy of the User.

The Access Manager then checks, within the limits of time and resources available:

- the availability of data through other routes, such as colleagues of the User, who can make them available independently: in particular, the User can communicate in advance, by mail, to his/her Manager a reference colleague, with whom to check the possibility to collect the necessary data without activating the Emergency access procedure to data;
- that the User is not actually able to make them available autonomously in due time, and tries in particular, within the limits of time and resources available, to contact the User through the available channels (e.g.: telephone) and informs him/her, if possible, of the intention to use the emergency access to data procedure.

If, at the end of these checks and evaluations, the Access Manager deems it necessary to use the emergency access to data procedure, s(he) will start the procedure and report the following information in the Minutes:

- the type of data to be accessed and the areas in which they will be searched (e.g.: e-mail, PC, etc.);
- an assessment of the need related to the access and possible impacts on the Foundation in case of non-access;
- an assessment of the possible impacts on the User in case of access;
- the actions that have been carried out to try to find the data through other methods and to contact the User;
- The attempts made to contact the User and - if it was successful - any objections or considerations made by the User related to the possible access.

Where possible, the Manager of the ICT Directorate identifies in advance the methods of access to the different IT tools (e-mail, PC, etc.) effective in ensuring their data availability, which minimize the impact on the User's privacy. Where the information must be searched in several User's IT tools, and unless there are specific reasons for a different search order (for example, the probability that the information is in one or other IT tool), the preferred search order is:

- Storage on premises;
- PC;
- Cloud Services;
- E-mail.

The ICT Manager appoints a competent System Administrator to support the Access Manager in carrying out the Emergency Access to data Procedure, always working together with the Access Manager.

Under no circumstances, will the Access Manager access the User's data independently. The activities must be carried out in a proper confidential environment, excluding persons not included in this activity, to protect the User's privacy.
In carrying out the search, the System Administrator will restrict the search to the data strictly necessary to achieve the purpose of the activity. The search methods will be different for each IT tool. Below, are the main IT tools.

a. Folders on storage on premises

The System Administrator, together with the Access Manager, accesses the folders stored on the premises using his/her administrative credentials. The Access Manager provides the System Administrator with all the information necessary to identify the data to be accessed (for example, project names, file names, dates) to minimize the need to access other data. The System Administrator will look for these data and will select search methods that reduce access to non-relevant data (e.g.: file search tools, folders and file contents based on keywords, rather than browsing the contents of folders and files).

b. Personal Computer

The System Administrator, together with the Access Manager, accesses the PC of the User using his/her administrative credentials. The Access Manager provides the System Administrator with all the information necessary to identify the data to be accessed (for example, project names, file names, dates) to minimize the need to access other data. The System Administrator will then look for these data and will prioritise search methods that reduce access to non-relevant data (e.g.: file search tools, folders and file contents based on keywords, rather than browsing the contents of folders and files). In carrying out the search, the System Administrator will identify the folders that, in line with the ICT Policy, the User will have made clearly recognizable as "for personal use" and will exclude these folders from the search.
If the System Administrator does not have the credentials to access to the User's PC, s/he may, as appropriate:
- access the PC through an external boot disk;
- remove the hard disk to access it from another PC.

If access to the hard disk is not possible through these simple methods, for example because the data or disk are encrypted, any recovery attempts must be made on a copy of the data, to minimise the risk of irretrievably damage or lose on the original data.

c. Cloud services provided by the Foundation

The System Administrator, together with the Access Manager, identifies the method to access to the cloud services assigned to the User. The methods of access may vary depending on the type of service, and may include, if necessary, resetting of the User's password and the access to related e-mail box, through the method described below, to obtain the information sent by the cloud service as part of the password reset procedure. Any new defined passwords will be chosen and stored by the System Administrator. These passwords will not be provided to the Access Manager.
The Access Manager provides the System Administrator with all the information necessary to identify the data to be accessed (for example, project names, file names, dates) to minimize the need to access other data. The System Administrator will search for these data and selecting search methods that reduce access to non-relevant data (e.g.: using file search tools, folders and file contents based on keywords, rather than browsing the contents of folders and files).

d. E-mail

The System Administrator, together with the Access Manager, identifies the most appropriate method to access to the e-mail folders.. This will enable a search of the messages based on sender, recipient, date, object or text. The Access Manager will provide the System Administrator with the parameters on which to base this search, to ensure this is undertaken in the most correct and specific way.
The System Administrator will identify a group of e-mail messages corresponding to the requirements defined, and will allow the Access Manager to view the parameters on the screen (sender, recipient, subject and date) where s/he can indicate which emails must be read to complete the search. The System Administrator and Access Manager will continue with the search until the necessary messages have been identified.

Once the searched for data have been identified, the System Administrator will extract it, for example by download to an external memory, and give it to the Access Manager.
At the end of the activity, the Access Manager will write in the Minutes the operations carried out and the list of extracted files together with a description of their contents. The System Administrator will sign the Minutes to verify the procedure/process. The Minutes, duly signed by the parties involved (see Process 1 below), will be forwarded by the Access Manager to the Human Resources and Organization Department, where the User, in future, can access this information.
. The Human Resources and Organization Department will then promptly notify the User via e-mail, where the procedures required to read the Minutes will be shown.

Process 1

#	Activity	Function	Input/Output
1	Evaluation of the need to access data, with length of absence period parameters that will activate the process.	Scientific director	I: Reporting of need to access data.
2	Evaluation of alternative ways to access the data (through collaborators or waiting for the User)	Access manager	I: Reporting of needs to access data.
3	Drafting of the minutes	Access manager	O: Minutes draft
4	Integration of Minutes and evaluation of the opportunity and how to continue	Access manager	I: Minutes draft O: Integrated Minutes
5	Identification of access method to systems	ICT Directorate (Director)	
6	Appointment of a System Administration	ICT Directorate (Director)	
7	Extraction and delivering of searched data	ICT Directorate (System Administrator)	O: searched data extraction
8	Registration and validation of the activities carried out and data extracted	Access manager/ICT Directorate (System Administrator)	I: Integrated Minutes

			O: Minutes validated
9	Notify the access to the user and define how the minutes will be shown	Human Resources and Organization Management	

5. Procedure: flow chart