POLICY FOR THE USE OF IT SYSTEMS

Read and approved on July 21st, 2008 – Modified on May 24th, 2010

Updated version of November 28t, 2011, Updated version of 05.17.2013

Introduction

The IT and telephone resources provided by the Foundation constitute one of the strengths of the FBK research centres, but at the same time they can pose risks to the security of the information being processed and the FBK's image. For this reason, use of these resources must always be guided by the principles that normally underpin professional relations such as diligence and fairness..

The creation of clear and precise rules for the use of the FBK's IT tools by employees and collaborators is an essential element in the process of optimising the Foundation's operations. The development of an ethical code to govern relations with internal staff, containing reciprocal guarantees between the parties, is indispensable for managing the legal and managerial problems that arise out of the activities and unintentional conduct that can lead to problems or threaten security in data processing.
These are the elements which the Foundation has drawn upon in drafting the code of conduct, in accordance with prevailing legislation, the principles of justice and the guarantee of the rights of the individual. An understanding of the reasons behind codes of conduct will lead to them being respected spontaneously.

These requirements form part of the specific instructions already given to all persons in charge of data processing, in implementation of Legislative Decree no. 196/03 as amended, concerning the processing of personal data and minimum security measures, and comply with the provisions of the Measure from the Privacy Guarantor of 1 March 2007.

The protection of workers

The workplace is a social sphere in which it is essential to protect the rights, fundamental freedoms and dignity of those who work there in order to guarantee, within a framework of reciprocal rights and responsibilities, the free expression of the personality of workers and ensure reasonable protection of their confidentiality in personal and professional relations.

Rights to the protection of personal data

In setting out the following rules the Bruno Kessler Foundation has taken into account the right to protection of personal data and the need for processing to be managed so as to provide a high level of protection for people, as well as the principles of simplification, harmonisation and effectiveness (Articles 1 and 2, Legislative Decree no. 196/03 as amended - the Personal Data Protection Code). These rules may be updated in light of experiences and technological innovation. Processing shall comply with guarantees concerning data protection and will be carried out in accordance with the principles of necessity and fairness, for specific, explicit and legitimate purposes, and will be relevant, not excessive and conducted in the least invasive manner possible.

Principle of transparency

Based on the principle of fairness, the Bruno Kessler Foundation has created this policy document in a spirit of transparency, as provided for in the rules for the sector (Article 4 (2), Workers' Statute; Legislative Decree n. 81/08 as supplemented and amended, concerning the "use of equipment fitted with video display terminals").

POLICY FOR THE USE OF IT SYSTEMS

I - Introduction

The information systems used by employees and collaborators are work instruments owned by the Bruno Kessler Foundation.

II - Purpose

The purpose of this policy is to ensure the information systems in the FBK are used correctly. These rules are intended to protect the FBK, its employees and collaborators, from the risk of systems and network services being compromised, from the disclosure of confidential personal data, and from the associated legal consequences, as well as making the use of information systems more effective.

III - Intended audience

This policy document is aimed at anyone with a formalised relationship with the Foundation (employees, collaborators, scholarship holders, those writing graduation theses, etc.) and who need to use any information system owned by or at the disposal of the Foundation. These people will be referred to below as "users".
The following provisions will also make reference to the positions provided for by Legislative Decree no. 196/03 as amended, namely the Data Controller, the Data Processor and the person in charge of the processing of personal data, as identified in the Security Policy Document.

IV - Operational methods

A - Use of equipment

1. Equipment provided by the Foundation is to be used for professional purposes. In deviation from this principle, the Bruno Kessler Foundation permits moderate and reasonable private use. Such use must be limited and based upon common sense and must not obstruct professional use. Space on the equipment used for "private" purposes (for example transferring files, photographs or videos) must therefore be limited and must not preclude and limit professional use.
2. Network drives, for example file servers, must be used solely for sharing work-related information and may not be used for other purposes under any circumstances. Therefore these drives may not be used to transfer non-work related files, even for short periods, as these drives are regularly used by System Administrators to conduct checks, administrative activities and backups.
3. In order to safeguard their privacy, users must create a folder in their email mailbox called "personal mail", to which all "private" messages must be transferred. This folder will not be checked by Network Administrators in any way.
4. Access by means of personal IT devices, for networks that allow it (see point 1 of Part E - Implementation), may take place on condition that provisions under paragraph B - Compliance with the provisions of Law - are fully respected.
5. The Foundation, in compliance with environment protection policies, has always engaged in energy saving programs and the correct use of IT instruments contributes to the achievement of such objectives. To that end, users will make sure that the IT devices used by them within the premises of the Foundation are configured in accordance with the following rules:
    a. personal computers will be automatically turned off or put into standby mode or hibernate if not used for more than an hour unless motivated research needs require so;
    b. the monitor will be automatically switched off or put in stand-by mode if not used for more than 5 minutes

B - Compliance with legal requirements

1. Use of the Foundation's equipment is subject to legal restrictions and the provisions of this policy. In particular, information systems may not be used in the following circumstances:
    a. in violation of the provisions of criminal, civil and administrative law;
    b. for uses that are incompatible with the objectives and institutional activities of the FBK;
    c. for unauthorised access to networks inside or outside the FBK;
    d. for activities that breach the confidentiality of other users or of third parties;

e. for activities that have a negative impact on the normal operations of the network or resources (e.g. people, skills, processing) or that compromise usability and performance;
f. for activities that result in the unauthorised transfer of information;
g. for activities that break the laws for the protection of intellectual property;
h. in violation of the Accettable use policy of the GARR network (annex D);

and uses that violate the provisions of these policies in any way.

2. All workstations connected to FBK networks must comply with the security measures provided for by Articles 31, 33 - 36 of Leg. Decree 196/03 as amended (Privacy Code), and in particular by the minimum measures laid down in Annex B. On this, see Appendix B

C - Data management and protection

1. The principal network servers are backed up by System Administrators, as described in the Security Policy Document and in the Service Charter. Users who store Bruno Kessler Foundation data in areas for which the Security Policy Document does not require a backup are responsible for backing up this data themselves and will be held liable for any damages incurred by the Foundation or by third parties, including civil damages, caused by its loss or theft.
2. Without prejudice to the existing measures to protect the privacy of staff, users must be aware that the data they process on the Foundation's information systems may be the property of the Foundation or in any case may fall within its responsibility. In order to guarantee the security and integrity of the information on the FBK's computer systems, FBK cannot provide an absolute guarantee of the confidentiality of information in the event of inspections.
3. Mailboxes may be opened in the event of unexpected or prolonged absences and due to unavoidable work-related requirements through a delegation provided by the FBK to "trustees". These trustees will inspect the contents of messages and forward those messages deemed relevant for the fulfilment of the professional activity to the Data Controller. The Bruno Kessler Foundation has designated the Data Processors (for their respective departments) and the System Administrators as the trustees for the entire organisation. This designation complies with the provisions of the Measure from the Privacy Guarantor of 1 March 2007 concerning the use of the internet and email. Trustees are expressly forbidden from accessing users' personal mail folders in their absence.
4. For the purposes of protection of privacy, the user can alert their recipients of the potentially non-confidential nature of the message through the following disclaimer: "The nature of this message is non-personal and FBK might become aware of any replies."
5. In the event the person in charge of the processing no longer occupies this position or leaves the Foundation, the following operational rules apply:
   a. The credentials for accessing the systems and email will be withdrawn.
   b. Their mailbox will be configured to continue receiving messages for around 4 months.
   c. The Foundation may decide to archive work-related emails from the mailbox of users that no longer belong to the organisation. However, messages in the personal mail folder will be deleted immediately.

   These activities are performed by System Administrators authorized to handling e-mail, who will therefore have access, due to exclusive technical reasons and only where it is not avoidable, to personal data stored in the mailbox.

D - Control Activities

1. As provided for by the Measure from the Privacy Guarantor of 1 March 2007, System Administrators are instructed by the Data Controller to conduct non-personal checks on the network and all equipment within it. The details of the inspections conducted are available in Appendix E.
2. For the correct maintenance of the systems and in order to guarantee their security, System Administrators may monitor tools, systems, network traffic and the use of resources at any time, including on a periodic basis, while ensuring all efforts are made to safeguard the privacy of users.
3. Under no circumstances will secret checks be carried out on individuals. Initial checks, relating to operations considered damaging and that in any case are unauthorised, will be applied across the board to all users. Should unauthorised activities persist, the Foundation will be justified in narrowing the focus of its inspections by conducting checks at the level of homogenous groups. If these checks determine additional abuses and behaviour that may compromise the security of information systems, that are

damaging to the organisation's assets or that constitute criminal offences, steps will be taken to identify the persons involved.

4. The Foundation is nevertheless required to notify the judicial authorities of all illegal conduct, including when determined through analysis conducted without identifying individual users.
5. At any time System Administrators may conduct targeted removals of files or applications deemed dangerous to the security of workstations or network drives.

E - Implementation

1. The Foundation provides users with different types of networks:
    a. Trusted, restricted to centrally-managed computers owned by the Foundation;
    b. Untrusted, restricted to privately-owned computers or FBK computers not managed centrally;
    c. DMZ, for centrally-managed servers that provide external services.
2. When any equipment is connected to the FBK network for the first time, this must be authorised explicitly by System Administrators.
3. System Administrators are the only persons with access to managed information systems connected to the FBK trusted and DMZ networks with Administrator or Root User privileges, whether local or network. During periods when a user is on travel away from the Foundation, their local privileges may be increased on a laptop provided by the Foundation. Without exception, the machine on which access privileges are modified must be restarted and reinstalled.
4. In order to ensure maximum flexibility for research purposes, at the explicit request of the user and subject to authorisation by their head of department, it may be possible to transfer all responsibility for management of an FBK laptop to the user. Computers configured in this way may not be connected to the FBK trusted networks. When choosing to use a computer in this way the user must sign a document (Annex A) through which they are designated the Data Processor, and are therefore subject to the civil and criminal liability associated with this position, particularly concerning Legislative Decree no. 196/03 as amended (Privacy Code). These users will be given preparatory and periodic training, as required by prevailing legislation, in order to provide basic knowledge of minimum security measures (Annex B) and the general obligations provided for by the Privacy Code.
5. It is forbidden to make any modifications to the operating system or the applications installed by System Administrators on the FBK trusted networks and centrally-managed workstations.
6. Users must keep their own passwords secret and may not share accounts. All users are responsible for security and any operations conducted using their own credentials. It is forbidden to access the network and programs anonymously or with someone else's credentials.
7. Users' passwords must be changed at least every six months. The passwords of persons in charge of processing sensitive data must be changed at least every three months. Passwords with high level privileges (root users, administrators, system administrators, etc.) must be changed at least every three months. This does not apply to passwords that have been authorised in advance purely for technical administration and which are generally used sporadically.
8. Access from outside the Foundation's network is only permitted through precise secure connection methods, indicated by the System Administrators in the Service Charter. Any other access is strictly forbidden.
9. The use of High Performance Computing Systems (HPC) are subject to the additional rules described in Annex C.

V - Liability

Anyone who fails to respect these policies may be immediately denied access to information systems by the System Administrators, who will notify the relevant Data Processor.

System Administrators are also obliged to inform the head of the HR Business Partner Department about any violations, for the purpose of initiating possible disciplinary proceedings.

It should be noted that breaches of the security rules imposed by Legislative Decree no. 196/03 as amended may involve additional independent consequences of a civil and criminal nature.

ANNEX A
Letter of Liability for the Processing of Personal Data

Purpose: Appointment of Data Processor (pursuant to Article 29 of Legislative Decree no. 196/03)

Dear Mr/Mrs_____,

Given your duties and in view of your proven experience, capabilities and reliability, the Bruno Kessler Foundation, in its capacity as the Data Controller pursuant to Legislative Decree no. 196/03, "Personal Data Protection Code" (hereinafter the "Code"), hereby appoints you, pursuant to Article 29 of the Code,

Data Processor

entrusting you, until withdrawal, with the tasks attributed by law to this person.
This appointment concerns the processing of personal data contained in the electronic equipment provided to you, as per the attached list, entrusting you with the tasks attributed by law to this person, including the security profile and the respective measures provided for by law.
Within the scope of this assignment you are required to follow the instructions set forth below, which are provided in accordance with Article 29(4) of the Code:

- The collection, registration, organisation, conservation, consultation, preparation, modification, selection, extraction, comparison, use, interconnection, restriction, communication, divulgation, cancellation and destruction of personal data must take place in such a way as to guarantee respect for the rights, fundamental freedoms and dignity of the individuals involved, with particular reference to confidentiality and personal identity, as well as respect for the rights of legal entities and any other body or association;
- In particular, personal data must be:
  - processed lawfully and fairly;
  - collected and registered for specific, explicit and legitimate purposes and used in other processing operations in terms that are not incompatible with such purposes;
  - accurate, and if necessary, up to date;
  - relevant, complete and not excessive in relation to the purposes for which they have been collected and subsequently processed;
  - maintained, in a format that allows the identification of the interested party, for no longer than is necessary for the purposes for which the data was collected or subsequently processed.

With regard to the protection of the "interested parties", namely the persons to whom the data refers, the Data Processor is responsible for:

- ensuring that the individuals, legal entities, bodies or associations to which the personal data refers, as well as the person from whom the personal data is collected, are informed in advance of the purpose, procedures and meaning of the data processing, according to the provisions of Article 13 of the Code, and have validly given their consent, when required, pursuant to Article 23 of the same Code;
- permitting the interested parties to exercise the following rights afforded them by the Code:
  - to obtain confirmation of whether personal data relating to them exists, even if not yet registered, and to have this data communicated in an intelligible form;
  - to obtain an indication of:
    - the source of the data
    - the purposes and methods of the processing
    - the logic applied to the processing, if the latter is carried out with the help of electronic means
    - the identification details of the data controller and the Data Processors
    - the entities or categories of entities to whom or which the personal data may be communicated or who or which may become aware of said data in their capacity as Data Processors or persons in charge of the processing.
      - to have the data updated, rectified, or where interested therein, supplemented;

- to secure the deletion, anonymisation or blocking of data that has been processed unlawfully, including data whose retention is unnecessary for the purposes for which it has been collected or subsequently processed;
- to obtain certification to the effect that the operations as per the previous two points have been notified, as also related to their contents, to the entities to whom or which the data was communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected

The Data Processor must also guarantee the right of the interested party to object, in whole or in part:

- on legitimate grounds, to the processing of personal data concerning him/her, even though it is relevant to the purpose of the collection;
- to the processing of personal data concerning him/her where it is carried out for the purpose of sending advertising materials or direct selling or else for the performance of market or commercial communications surveys.

In your capacity as Data Processor you must comply with the provisions of Articles 26 and 27 concerning sensitive and judicial data, and in any event honour the requirements given by the Guarantor or by the Judicial Authority concerning the processing of personal data, promptly informing the Data Controller of any relevant question for the purposes of the law.

Concerning the fundamental requirement to guarantee the security of all data processed, you must adopt the measures provided for by Annex B to the Code in order to prevent data from being disclosed or destroyed, and above all to prevent data from being accessed by unauthorised persons, or being processed in an unauthorised manner or in ways unconnected with the purpose for which it was collected, including by personnel with authorisation to access it.
In any event, you must guarantee that current security standards are maintained and not lowered in relation to the purposes indicated above.

The company, as Data Processor, is available to provide any additional information, training, documentation and support that may be of use for the completion of the tasks specified above.
Moreover it should be noted that, pursuant to Article 29 of the Code, the Data Controller is required to ensure, including by means of periodic checks, that the appointed Data Processors observe the instructions given, without prejudice to the rules in place to protect the dignity of workers.
By signing this document you accept the position and acknowledge the instructions given (Policy for the use of information systems - point IV operational procedures - Letter E implementation - point no. 4).

Trento, _____ Inventory Number _____

The Data Controller

_____

The Data Processor

_____

The Unit Head/Director

_____

Annex B
Security Measures under the "Privacy Code" (Legislative Decree 30 June 2003, n. 196)

Art. 31. Safety obligations
1. Personal data undergoing processing are protected and controlled, even in relation to knowledge acquired on the basis of technical progress, to the nature of the data and to the specific characteristics of the processing, so as to reduce to a minimum, through the adoption of suitable preventive security measures, the risks of destruction or loss, even accidental, of data, of unauthorized access or of processing that is not allowed or not in accordance with the purposes of the collection.

Art. 33. Minimum measures
1. In the context of more general security obligations referred to in Article 31, or covered by special provisions, the officers entitled to the processing are still required to take the minimum measures identified in this Decree or under Article 58, paragraph 3, aimed at ensuring a minimum level of protection of personal data.

Art. 34. processing with electronic means
1. The processing of personal data carried out through electronic means is permitted only if the following minimum measures are taken in the manner prescribed by the technical specifications set out in Annex B):

a) computerized authentication;

b) establishment of procedures for the management of authentication credentials;

c) use of a permit system;

d) periodic updating of the identification of the processing allowed to each officer in charge of the management or maintenance of electronic instruments;

e) protection of electronic devices and data against unlawful processing of data, unauthorized access and some specific computer programs;

f) the establishment of procedures for storing backups, for restoring the availability of data and systems;

g) [deleted] (1);

h) the adoption of encryption techniques or identification codes for the processing of specific data disclosing health and sex lifestyle made by health organizations.

1-bis. [repealed] (2)

1-ter. For the purposes of applying the provisions regarding the protection of personal information, the processing operations for administrative and accounting purposes are those related to the activities of organizational, administrative, financial and accounting nature, regardless of the nature of the information processed. In particular, such objectives are pursued by internal organizational activities, that are functional to the performance of pre-contractual and contractual obligations, to the management of the employment relationship in all its phases, to accounting activities and to the application of regulations related to taxes, trade unions, social security and welfare, health, occupational hygiene and safety. (3)

Article 35. Processing without the aid of electronic instruments
1. The processing of personal data carried out without the aid of electronic instruments is allowed only if the following minimum measures, in the manner prescribed by the technical specifications set out in Annex B), are taken:

a) regular update of the scope of the permitted processing to individual agents or organizational units;

b) implementation of procedures for proper storage of records and documents entrusted to the officers in charge for the performance of their duties;

c) implementation of procedures to keep specific records in limited-access archives and definition of an access procedure in order to identify officers in charge.

(1) Letter abolished by.art. 45, paragraph 1, lett. c) of Leg. D. n. 5 dated 9 February 2012, , retified with amendments, by Law n. 35 dated 4 April 2012,. It shows, for completeness, the original text, "maintaining an updated planning document on security."
(2) Paragraph added from art. 6, paragraph 2, letter. a) number 5) of Leg. Decree n. 70 dated 13 May 2011, retified with amendments, by Law n. 106 dated 12 July 2011, (replacing the previous paragraph 1-bis added by art. 29, paragraph 1 of Leg. Decree n. 112 dated 25 June 2008, ratified with amendments by Law n. 133 dated 6 August 2008) and subsequently repealed by art. 45, paragraph 1, lett. c) of Leg. Decree n. 5 dated 9 February 2012, , ratified with amendments by Law n. 35 dated 4 April 2012,.
(3) Paragraph added by.art. 6, paragraph 2, letter. a) number 5) of Leg. Decree n.. 70 dated 13 May 2011, ratified with amendments by Law n. 106 dated 12 July 2011, replacing the previous paragraph added by Article 1-bis. 29, paragraph 1 of Leg. Decree n. 112 dated 25 June 2008, , ratified with amendments by Law n. 133 dated 6 August 2008,.

Annex B to Legislative Decree no. 196/03
(Articles 33 to 36 of the Code)

Processing by electronic means

Technical arrangements to be implemented by the Data Controller, the Data Processor where appointed and the person in charge of the processing, in the event of processing by electronic means:

Computerised authentication system

1. Persons in charge of the processing shall be allowed to process personal data by electronic means if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations.
2. Authentication credentials shall consist in an ID code for the person in charge of the processing as associated with a secret password that shall only be known to the latter person; alternatively, they shall consist of an authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password.
3. One or more authentication credentials shall be assigned to or associated with each person in charge of the processing.
4. The instructions provided to the persons in charge of the processing shall lay down the obligation to take such precautions as may be necessary to ensure that the confidential component in the credentials are kept secret and that the devices used and held exclusively by persons in charge of the processing are kept with due care.
5. Where provided for by the relevant authentication system, a password shall consist of at least eight characters; if this is not allowed by the electronic equipment, a password shall consist of the maximum permitted number of characters. It shall not contain any item that can be easily related to the person in charge of the processing and shall be modified by the latter when it is first used as well as at least every six months thereafter. If sensitive or judicial data are processed, the password shall be modified at least every three months.
6. An ID code, if used, may not be assigned to another person in charge of the processing even at a different time.
7. Authentication credentials shall be deactivated if they have not been used for at least six months, except for those that have been authorised exclusively for technical management purposes.
8. Authentication credentials shall be also deactivated if the person in charge of the processing is disqualified from accessing personal data.
9. The persons in charge of the processing shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during processing sessions.
10. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the Data Controller can ensure that data or electronic equipment are available

in case the person in charge of the processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities shall have to inform the person in charge of the processing, without delay, as to the activities carried out.

11. The provisions concerning the authentication system referred to above as well as those concerning the authorisation system shall not apply to the processing of personal data that is intended for dissemination.

Authorization System

12. Where authorisation profiles with different scope have been set out for the persons in charge of the processing, an authorisation system shall be used.
13. Authorisation profiles for each person or homogeneous set of persons in charge of the processing shall be set out and configured prior to the start of the processing in such a way as to only enable access to the data that is necessary to perform processing operations.
14. It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply.

Other security measures

15. Within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing as well as to the technicians responsible for management and/or maintenance of electronic equipment, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.
16. Personal data shall be protected against the risk of intrusion and the effects of programs as per Section 615-quinquies of the Criminal Code by implementing suitable electronic means to be updated at least every six months.
17. The regular update of computer programs as aimed at preventing vulnerability and removing flaws of electronic means shall be carried out at least annually. If sensitive or judicial data is processed, such update shall be carried out at least every six months.
18. Organisational and technical instructions shall be issued such as to require at least weekly data backups.

Security Policy Document

19. [deleted] (1)
19.1 [deleted] (1)
19.2 [deleted] (1)
19.3 [deleted] (1)
19.4 [deleted] (1)
19.5 [deleted] (1)
19.6 [deleted] (1)
19.7 [deleted] (1)
19.8 [deleted] (1)

Additional measures applying to processing of sensitive or judicial data

20. Sensitive or judicial data shall be protected against unauthorised access as per Article 615-ter of the Criminal Code by implementing suitable electronic means.
21. Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data is stored in order to prevent unauthorised access and processing.
22. The removable media containing sensitive or judicial data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorised to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means.
23. If either the data or electronic means have been damaged, suitable measures shall be adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days.
24. Health care bodies and professionals shall process data disclosing health and sex life as contained in lists, registers or data banks in accordance with the mechanisms referred to in Article 22(6) of the Code also in

order to ensure that said data is processed separately from the other personal data allowing data subjects to be identified directly. Data concerning genetic identity shall only be processed in protected premises that may only be accessed by such persons in charge of the processing and entities as have been specifically authorised to access them. Containers equipped with locks or equivalent devices shall have to be used in order to remove the data outside the premises reserved for their processing; the data will have to be encrypted for the purpose of electronically transferring it.

Safeguards and protections

25. Where a Data Controller adopts minimum security measures by committing the relevant tasks to external entities, prior to implementing such measures he or she shall require the installing technician(s) to supply a written description of the activities performed by which it is certified that they are compliant with the provisions set out in these technical specifications.
26. [deleted] (1)

Processing without electronic means

The following technical arrangements to be implemented by the Data Controller, data processor – if nominated – and person(s) in charge of the processing whenever data is processed without electronic means:

27. The persons in charge of the processing shall be instructed in writing with regard to controlling and keeping, throughout the steps required to perform processing operations, records and documents containing personal data. Within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.
28. If records and documents containing sensitive or judicial personal data are entrusted to the persons in charge of the processing for the latter to discharge the relevant tasks, said records and documents shall be kept and controlled by the persons in charge of the processing until they are returned so as to prevent unauthorised entities from accessing them; they shall be returned once the relevant tasks have been discharged.
29. Access to archives containing sensitive or judicial data shall be controlled. The persons authorised to access said archives for whatever purpose after closing time shall be identified and registered. If an archive is not equipped with electronic devices for access control or is not placed under the surveillance of security staff, the persons accessing said archive shall have to be authorised in advance.

(1) Paragraphs suppressed by art. 45, paragraph 1, lett. d) of Decree Law 9 February 2012, n. 5, ratified with amendments by Law 4 April 2012, n. 35.

For completeness, the following is the text of deleted paragraphs.

19. By 31 March of each year, the controller of processing operations concerning sensitive and/or judicial data shall draw up, also by the agency of the data processor, if nominated, a security policy document containing appropriate information with regard to:
19.1. the list of processing operations concerning personal data;
19.2. the distribution of tasks and responsibilities among the departments/divisions in charge of processing data;
19.3. analysis of the risks to which the data are subject;
19.4. the measures to be taken in order to ensure data integrity and availability as well as protection of areas and premises insofar as they are relevant for the purpose of keeping and accessing such data;
19.5. a description of the criteria and mechanisms to restore data availability following destruction and/or damage as per point 23 below;
19.6. a schedule of training activities concerning the persons in charge of the processing with a view to informing them on the risks applying to the data, the measures that are available to prevent harmful events, the most important features of personal data protection legislation in connection with the relevant activities, the resulting liability and the arrangements to get updated information on the minimum security measures adopted by the Data Controller. Said training activities shall be planned as of the start of the employment relationship as well as in connection with changes in the task(s) discharged and/or the implementation of new, significant means that are relevant to the processing of personal data;
19.7.a description of the criteria to be implemented in order to ensure adoption of the minimum security measures whenever processing operations concerning personal data are externalised in accordance with the Code;
19.8. as for the personal data disclosing health and sex life referred to under point 24, the specification of the criteria to be implemented in order to either encrypt such data or keep it separate from other personal data concerning the same data subject.

26. The Data Controller shall declare in the report accompanying the financial statements, whether due, the preparation or amendment of the security policy document.

Note: The foundation has decided to keep the Security Policy Document, despite its formal repeal of law n 4 April 2012. 45, since it is a list of the security measures taken pursuant to articles of law set out in this Annex.

Annex C
Additional rules for the use of HPC Systems

I – HPC Systems Users

1. All the contributing research units people can use HPC Systems at no additional costs. Users from one of such units can send an e-mail to gsc@fbk.eu to request access or support.
2. All the contributing research units heads will participate in the board called "Cluster-Strategic". This board will take strategic decisions about the future of HPC Systems
3. All contributing research units heads will elect one or two member of a second board called "Cluster-Technical". This board will take technical decisions about HPC Systems.
4. All other access requests should be addressed to Cluster-Strategic.

II – HPC Systems Usage

1. Users must use Secure Shell (ssh) tools to login into HPC Systems and Secure Copy Protocol (SCP) to transfer file from and into HPC Systems. The system will not accept incoming connections from any other protocols. Once users are logged into, outgoing connections will not be allowed for security reasons.
2. The machine in which users will be logged into will be named "Logon Server" and will act as a front-end. It may be used for editing, compiling/debugging of small applications and for preparation and submission of batch executions.
3. The execution of cpu-bound programs is strongly discouraged on the Logon Server. If some executables are CPU intensive (targz, compile and debug sessions, ect.), users must run them through the queue system.
4. Copying data inside or outside HPC Systems will be performed using SCP from an external file server to one of the internal file servers.
5. All jobs must be run through the queue system. Different type of queues will be available for different purposes.
6. It is not possible to connect directly to the compute blades from the login nodes: however, interactive sessions on specific blades can be achieved through the queue system.
7. Debug must be performed on a queue.
8. Every blade has a local hard drive that can be used as a local scratch space to store temporary files during executions of jobs. The amount of the scratch space varies from node to node. All data stored in these local hard drives at the compute blades will not be available from the other blades nor from the logon server. Users are strongly encouraged to copy the needed data for each job to the local scratch space at the beginning and copy it back to the file server at the end. All users data on the local scratch area must be deleted at the end of the job. **Every file older than one week, after a warning, will be automatically deleted.**

III – HPC Systems Resource allocation

1. Usually the HPC Systems blades are used in shared mode. Users in need of exclusive use of blades for an extensive period of time must use the provided shared calendar for booking, providing the estimated usage time and the estimated number of exclusive blades. Every group of users can book in exclusive mode a limited number of blades that will be reserved ASAP starting from the requested date and time.
2. At the time of job submission users must specify the maximum usage of RAM. One Gbyte of RAM will be reserved for Operating System and daemons. All jobs exceeding said limit will be killed.
3. The users are strongly advised to use checkpointed jobs.
4. Storage quotas on file servers are enforced at group level. Each group will have different quota limits.
5. Units in need of special jobs shall ask Cluster-Technical for a specific solution.

IV – Job monitoring

1. Email notifications will be sent to users for the important events involving their running jobs:
    a. Job killed (with reason)
    b. Job suspended (with reason)
    c. Job resumed
    d. Long running job
2. Users may choose to be notified by e-mail for the following events involving their running jobs:
    a. Job started
    b. Job accomplished.

Annex D
Acceptable Use Policy of the GARR Network

1. The Italian Scientific Research and Academic Network, commonly called "GARR Network", is based on scientific and academic collaboration projects between Italian public Universities, Italian public Schools and Scientific Organizations. Thereby the GARR network service is mainly addressed to all organizations that are under the authority of the Italian Ministry of Education, University and Research (MIUR). There is however the possibility of extending the service itself to other organizations that carry out research activities in Italy, in particular, but non exclusively, in the case of no-profit organizations that have collaboration activities with the Italian Ministry of Education, University and Research. All GARR users must anyway follow this Acceptable Use Policy (AUP) rules in order to access the nework service.
2. The "GARR Network Service", afterwards referred to as "GARR Network", is composed by the set of telematic connection services, network management services, application services and of all the interoperability instruments (done directly or on behalf of GARR) that enables authorized subjects to communicate among each other (national GARR Network). Integral parts of GARR Network are also telematic connections and services that enable the interconnection between the national GARR Network and the other Networks.
3. The following activities are not allowed on the GARR network:
    - To provide to not-authorized subjects network connectivity service or other services which include it, such as to provide housing or hosting services and alike, or to allow data or information routing on the GARR Network between two not-authorized subjects (third party routing).
    - To use network resources and services, to connect equipments or services or software to the network, to spread virus, hoaxes or other software in a way that can damage, trouble or disturb other people, other users or service activities available on the GARR Network and on any other networks connected to it.
    - To create and to send (if not for research purposes, and in any case in a quite controlled and legal way) any kind of image, data or other offensive item, libel or indecent documents that attack human's dignity, in particular for what regards sex, race or faith.
    - To send not required commercial and/or promotional documents ("spamming"), and to let third parties use one's own resources for this purpose.
    - To damage, destroy or to try to access data without authorization or to violate other users' privacy, to intercept or disseminate private passwords and cryptographic keys included.
    - To carry out on the GARR Network any other activity forbidden by the State Law, by the International rules and by the rules and netiquette of network and network services use.
4. The liability of published and disseminated documents content on the network is on people who publish and disseminate those documents. In case of people who are underage, the responsibility can also involve people who have their custody.
5. Authorized subjects (A.S.) to access GARR network, defined in the document "Approved rules by CRCS", can use the network for all one's own institutional activities. Institutional activities are defined as any activity related to the tasks provided for by the statute of an authorized subject, including activities of collaboration contracts or agreements approved by both involved parties, provided that these activities belong to the authorized subject institutional purposes. In particular institutional activities are: research activities, didactics, administrative tasks of the authorized subjects and between authorized subjects and research activities for third parties, with exclusion of all cases explicitly declared as not allowed in this document. Other subjects with a temporary authorized access to the network (T.A.) can carry out only the set of activities mentioned in their authorization. The final decision on the allowed activities on the GARR network is GARR Management Bodies' prerogative.
6. All authorized users must be known and identified. Therefore all possible measures must be taken to stop the access to not-identified users. As a rule users must be employees of authorized subjects, even if temporary. For what regards Authorized Subjects (A.S.), the users can be also people temporary authorized by them for an institutional job. Students who are regularly enrolled in a course by an authorized subject are admitted users.
7. It is responsibility of authorized subjects, even temporary, to adopt all reasonable actions to ensure the accordance of their own rules with the above mentioned ones and to ensure that forbidden actions do not happen on the GARR Network. Each authorized subject must let their own users know (by appropriate means they believe) the rules inside this document.

8. Authorized subjects, even temporary, to access the GARR Network explicitly accept that their names (name of the body, corporate name or corresponding) are put in an electronic database maintained by GARR Management Bodies.
9. In case of verified non-observance of these action rules, the GARR Management Bodies will take the necessary measures to bring back the network into its correct use, included the temporary or definitive suspension of the access to GARR Network itself.
10. The access to GARR Network is made conditional on the full acceptance of the rules inside this document.

Annex E
Details relating to control activities carried out by the System Administrators

The Foundation manages the computer systems and networks through tools that can temporarily store data related to internet browsing and network traffic. In particular, the following are listed:
:

1. Electronic mail - proper functioning of the system of message delivery and security anti-malware and anti-spam checks - stored data:
    a. log of SMTP traffic generated by the e-mail server;
    b. log of messages not forwarded correctly (delays and/or non-delivered);
    c. log of messages intercepted by the antispam system;
    d. log of messages intercepted by the antivirus system and subject to 30-day quarantine.

2. WEB Traffic – proper functioning of the system, SLA monitoring, security checks:
    a. log of http/https traffic generated on firewall devices. This log shall also include the navigation point data related to the internal IP of origin of the request. Data shall be kept for about 26 weeks in a system accessible only by authorized system administrators, and not normally used for other activities of the Foundation. However they might be stored for longer periods due to justified technical/organizational reasons, to ensure the exercise or defense of a legal action and in all cases where it is required by court authorities.

    Telephone system – proper functioning of the system:
    b. Log of calls (calling number, called number, duration).
3. Access to networks - proper functioning of the system, SLA monitoring and security checks:
    a. Log of remote access to the network.

The Foundation shall adopt backup procedures that protect against possible data loss. Currently, backups can contain:
- Data items from the folder “Pernal mail" that may have been created by the user, subject to the safeguards described in paragraph C - Management and data protection.
Copies currently stored allow to retrace data stored on FBK systems over the past 5 years.

As stated in the Guarantor Guidelines, the Foundation will not proceed in any case to not allowed email and internet checks, such as:
- Accurate reading and recording of e-mail messages;
- Reproduction and storage of the web pages you visit;
- Capture of typed characters through the keyboard (physical or virtual);
- Hidden analysis of personal computers entrusted in use.