FONDAZIONE
BRUNO KESSLER

Privacy Regulations
of Fondazione Bruno Kessler

Acceptable practices regarding the processing of personal and business information, ICT tools and systems

Approved with Resolution No. 15/17 dated December 20, 2017 of the Board of Directors

This document replaces and integrates the previous Policy on the Use of IT Systems in its latest version update of May 17, 2013

Amended with Resolution No. 08/19 dated January 29, 2019 of the Board of Directors

FONDAZIONE
BRUNO KESSLER

I. INTRODUCTION

1. PRELIMINARY REMARKS

Preserving the confidentiality, integrity and availability of data and information to protect the dignity of individuals, fundamental freedoms and the value of the Foundation's intellectual capital. This is the objective of these Regulations, which are part of the general regulation on Privacy, and of the regulatory system that governs the organization, processes and functions of the Foundation.

The IT and telecommunication resources made available by FBK are one of its strengths, but at the same time, they can be a source of risk to the security of the information processed and to the image of FBK itself. For this reason, their use must always be based on criteria of legality, correctness and transparency.

The identification of precise and clear rules for the use of IT tools and the processing of personal and corporate information represents a required step to ensure an optimal management of functions at FBK.

These are the elements that, in the context of the rules governing privacy, have prompted FBK to draw up, adopt, and update the present Regulations, which replace and integrate the previous Policy for the use of ICT systems in its latest version updated on May 17, 2013

2. PROTECTION OF WORKERS

The workplace is a social formation with respect to which the protection of the rights, fundamental freedoms and dignity of each person must be ensured in such a way as to guarantee, in a frame of mutual rights and duties, the explication of the worker's personality and a reasonable protection of its sphere of confidentiality in personal and professional relationships.

3. PURPOSE, SCOPE AND INTENDED AUDIENCE

The purpose of these Regulations is to define a set of practices, which all employees, collaborators, any third parties and - in general - internal and external people working for FBK must comply with in relation to the activities involving the processing of data and information.

These Regulations have been laid down in compliance with the provisions of European Directive No. 2016/679 - General Data Protection Regulation (hereinafter "GDPR"), of Legislative Decree n. 196/2003 - Code regarding the protection of personal data – (hereinafter “Code”) as amended and integrated by Legislative Decree No. 101/2018 - Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679, and the Provisions of the Data Protection Authority.

These Regulations apply to the following Users (hereinafter “Users”):

Internal Users:

- Members of the statutory bodies
- Employees
- In-house consultants
- Staff assigned to FBK premises
- Province employees assigned to work at FBK premises
- Occasional consultants
- Affiliates (High profiles, Affiliated fellows, Visiting fellows, PhD sudents, Scholars, High School interns).

External Users:

- Staff, in any capacity, of contractors providing supplies, services, or works for FBK and their employees or collaborators
- Staff of other organizations present at FBK due to MoUs or inter-institutional agreements
- Various visitors and guests

II. DEFINITIONS

1. Please see the main definitions concerning privacy below.

Personal data: any information that identifies a natural person or makes him/her identifiable and that may provide details as to their physical, physiological, genetic, mental characteristics, their habits, life style, personal relationships, their health conditions or economic status.

Identifying data: personal data that allow the identification of a natural person.

Particular data (former sensitive data): personal data suitable for revealing the state of health (relating to physical or mental health, including the provision of health care services) and sexual life, racial and ethnic origin, religious beliefs, philosophical or other beliefs, political opinions, membership in parties, trade unions, religious or philosophical associations, political or trade union organizations of a natural person.

Genetic data: personal data relating to the inherited or acquired genetic characteristics of a natural person, which give unique information about his/her physiology or health.

Biometric data: personal data resulting from specific technical processing relating to the physical, physiological or behavior characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Judicial data: data suitable for the collection of information regarding measures relating to criminal records, the register of administrative penalties related to the offense and the related pending charges, or the status of defendant or suspect in accordance with articles 60 and 61 of the criminal procedure code.

Processing of personal data: any operation performed with or without the use of automated processes and applied to personal data, or sets of personal data, such as collection, registration, organization, structuring, storage, adaptation, the modification, extraction, consultation, use, communication by transmission, diffusion or any other form of making available, comparison or interconnection, limitation, cancellation or destruction.

Profiling: any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects of professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movement of that physical person.

Pseudonymization: processing of personal data in such a way that personal data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is stored separately and subject to technical and organizational measures to ensure that such personal data are not attributed to an identified or identifiable natural person.

Disclosure of personal data: giving knowledge of personal data to one or more specific Users other than the interested party, on the basis of a specific purpose and a certain and safe method of processing, including by making available or consulting them.

Dissemination of personal data: giving knowledge of personal data to indeterminate Users, in any form, including by making available or consulting them.

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2. Please see the definitions concerning privacy Users below

Data Subject: is the individual whom particular personal data is about

Data Controller: The Foundation as a whole, in the person of its Legal Representative who exercises completely independent decision-making power over the purposes and methods of processing, including the security profile.

Joint Controller: Data controller who jointly determines the purposes and means of processing in a transparent manner and through an internal agreement, the respective responsibilities regarding compliance with the obligations deriving from the GDPR.

External Data Processor: natural or legal person, public authority, service or other body that processes personal data on behalf of the Data Controller. The External Data Processor must provide sufficient guarantees to put in place suitable technical and organizational measures so that the processing meet the requirements of the GDPR and guarantee the protection of the rights of the data Subject.

External sub-Processor: a natural or legal person, public authority, service or other body to which a Data Processor recurs for the execution of specific processing activities on behalf of the Data Controller;

Internal Data Processor: User, within the Foundation, who is entrusted with the responsibility for the processing of personal data attributable to his/her relevant area of concern. This User coincides with a Head of organizational articulation.

Authorized Data Processor: User, within the Foundation, authorized to perform data processing operations on the basis of the regulations adopted by the Data Controller and the instructions given by the Data Processor and/or by the Internal Data Processor.

System Administrator: natural or legal person appointed by the Controller and responsible for the management and security of information systems through the application of the necessary measures to maintain the confidentiality, availability and integrity of the personal data processed.

FBK-owned ICT tools Administrator: a natural person, within the Foundation, who autonomously manages ICT tools owned by the Foundation and who provides sufficient guarantees to put in place suitable technical and organizational measures so that the processing meets the requirements of the GDPR and ensures the protection of the rights of the data Subject and data of which FBK is the Controller.

Data Protection Officer (DPO): a natural person appointed by the Controller who, pursuant to art. 37-39 of the aforementioned GDPR, operating independently from the organization, advises the Controller regarding obligations, requirements and regulatory developments, carries out internal audits on the correct application of the regulatory provisions and the privacy management system defined by the Controller, assists the Controller with the privacy impact assessment and risk analysis, and represents the point of contact for data Subjects and Data Protection Authority.

3. The following are some other definitions useful for the correct management of the processing of personal data.

Badge: card with electronic recognition chip.

Pass: paper card without identification.

ICT tools: printers, laptops, desktop computers, landlines, smartphones, tablets, e-book readers, IP cameras, and, in general, any device that can connect to an IP network.

Data Center: a limited-access area hosting servers, computing systems and networking devices, as well as storage systems on which data are stored.

Public Cloud: data storage model on networked computers where the data is stored on multiple virtual servers generally hosted at third-party facilities or on dedicated servers.

III. ORGANIZATIONAL MODEL

1. INFORMATION CLASSIFICATION

FBK's information assets (consisting of all the data and information processed in the various processes, including personal data) can be classified according to the following criteria:

Public data and information: this information is freely traceable by Users through the means of communication made available by FBK (website, publications, press releases, etc.). This information does not require particular attention to confidentiality from the User. Disclosure of this information has no implications for FBK as it is public information that can be disseminated.

Internal data and information: this is information that can be processed by Users exclusively within the FBK processes and organizational context through the institutional channels made available by FBK (e-mail, intranet, website, areas of exchange on servers and computers, etc.). This information requires the User to pay special attention to the processing, as its disclosure is a violation of the confidentiality constraints to which each User is bound with a possible legal impact (e.g., breach of privacy), unless it is revised so that it is reclassified as public.

Confidential data and information: this is information that can be processed by groups of Users authorized by virtue of the role and a specific processing purpose identified by the Data Controller or the Data Processor. Such information must be disclosed only to entitled Users, evaluating the most appropriate communication tool made available by FBK as their dissemination can have a major legal (e.g. breach of privacy), image and competitiveness impact for FBK.

Strictly confidential data and information: it is information that can only be processed by certain Users based on the role and responsibilities covered in FBK. Disclosure of such information may result in serious legal (e.g. breach of privacy), image and competitiveness damage to FBK.

2. ORGANIZATIONAL MODEL OF LIABILITY FOR PRIVACY ISSUES

In compliance with the GDPR, FBK has defined and formalized an Organizational Model of privacy related liability aimed at the correct processing of personal data. The model is in line with the Foundation's organizational chart.

On the occasion of the annual update of the general organization chart, the Foundation, in its capacity as Personal Data Controller, also updates the line of internal responsibilities regarding the processing of personal data by identifying in the Managers of organizational articulations, regardless of their names (e.g. Centers, High Impact Lines/Areas, Units, Services, ...) the Internal Data Processors for personal data relating to processes of their concern solely. These Users are formally appointed after receiving specific training.

All those who are in charge of a project that involves the processing of personal data and have not been included in the Privacy-related Liability Organizational Model - are required to adopt an ad hoc policy tailored on the specific needs of the case (so-called Privacy by Design). These Users shall adopt the above policy in agreement

with the Data Controller and through the Corruption Prevention, Transparency and Privacy Unit including as well the Data Protection Officer.

3. FBK AS EXTERNAL DATA PROCESSOR

By virtue of the stipulation of contracts, agreements, projects with external parties, the Foundation can be appointed as "External Data Processor pursuant to Article 28 of the GDPR" when it is entrusted with specific tasks, which involve personal data processing for the specific purposes of a subcontractor (which is the Data Controller therof).

In all these cases, the Foundation - even when signing the aforementioned deeds – shall identify the Internal Data Processor.

4. RECORD OF PROCESSING ACTIVITIES

The Record of Processing activities is a document for the recording and analysis of the processing activities performed by the Data Controller. The Record must be promptly completed and kept constantly updated by each Internal Data Processor as its content must always reflect the effective processing activities performed. Any change, in particular in relation to the methods, purposes, categories of data, categories of data Subjects, must be immediately reported in the Record, and provide the reason for the changes occurred.

IV. ACCEPTABLE PRACTICES POLICY

1. PROCESSING MAIN PRINCIPLES

Personal data processing is any operation or set of operations performed on a personal data including those carried out without the aid of electronic tools. The processing of personal data, to be lawful, accurate and transparent must always take place according to some general privacy principles, which can be considered inseparable constraints to the processing of personal data. It is important to always ask ourselves if these constraints are being respected and only in case of an always positive answer can we be sure that the privacy of a person is ensured. In particular, when processing personal data, users are required to observe the following general principles:

- Dignity of the Data Subject, i.e. the natural person whom the personal data is about
- Lawfulness, accuracy and transparency: personal data must be processed in a lawful, accurate and transparent way, in order to guarantee to the Data Subject adequate security, including protection, through appropriate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage. With regard to transparency, all information intended for the public or to the Data Subject must be concise, easily accessible and easily understood; the language used must be simple and clear.
- Purpose limitation: the purposes of the processing must be certain, explicit and legitimate, and subsequently processed in a way that is not incompatible with such purposes (without prejudice to further processing for archiving purposes in the public interest or for scientific or historical research purposes; or for statistical purposes).
- Data minimization: the data collected must be adequate, relevant and limited to what is necessary with respect to the purposes for which they are processed. Specifically, information systems and computer programs must be configured by minimizing the use of personal data, so as to exclude their processing

when the purposes pursued in individual cases can be achieved through anonymous data or other appropriate ways to identify the data Subject only in case of necessity ('necessity principle').

- Accuracy: the data processed must be accurate and, if necessary, updated, therefore all reasonable steps must be taken to delete or edit inaccurate data in relation to the purposes for which they are processed.
- Retention limit: the data processed must be stored in a form that allows identification of the data Subject for a period not longer than the necessary to achieve the purposes for which they are collected and processed (unless specific law providing for archiving processing in the public interest or for scientific or historical research purposes, or for statistical purposes).
- Integrity and confidentiality: the data must be processed in such a way as to guarantee adequate security of personal data, including protection, by means of appropriate technical and organizational actions, from unauthorized or unlawful processing, loss, destruction and accidental damage.

2. PROCESSING OF PERSONAL DATA FOR STATISTICAL AND RESEARCH PURPOSES

Cultural activity and research are important ways to broaden the boundaries of knowledge, foster the growth of individuals' personalities and enable social progress.

To ensure these purposes, the processing of personal data may be permitted. In this context, the regulations governing the processing of personal data include simplified measures in the field of historical, scientific and statistical research. However, these measures do not exempt the Data Controller from adopting suitable measures to prevent possible violations of the rights of the data Subjects. In fact, the informed consent forms that are provided to the data Subjects, shall clearly explain and disclose the aims pursued by the statistical or research investigation.

Personal data processed for statistical and scientific research purposes cannot be used to make decisions or provisions concerning the data Subject, nor for processing for other purposes. They are stored separately from any other personal data processed for purposes that do not require their use.

The provisions, relating to the statistical secrecy and confidentiality of personal data, do not apply to data from public records, lists, deeds or documents that can be accessed by anyone.

In order to promote and support research and collaboration in the cultural, scientific and statistical fields, the Foundation – excluding particular and judicial data - can disclose and disseminate data related to study and research activities.

The Foundation's research staff is required to standardize its research and study activities to the ethical rules promoted by the Data Protection Authority[1] and that can be found in the Annex to the Foundation's Code of Conduct.

3. PUBLICATION OF DEEDS AND DOCUMENTS AND THE RIGHT TO PERSONAL DATA PROTECTION

The Foundation ensures the right to privacy for particular/judicial data contained in the documents published on the Transparent Administration webpage and on the institutional website, through non-direct identifiability of the data Subjects to whom these data refer, or through data hiding.

[1] https://www.garanteprivacy.it/web/guest/home_en/italian-legislation

4. ACCESS RIGHT VS PROTECTION OF PERSONAL DATA

The conditions, procedures, limits for the exercise of the right to access administrative documents containing personal data and the relative judicial protection are governed by Law 241/1990 as amended and integrated. and by the other regulatory provisions on the Subject, as well as the legislation on transparency governing the right of access, including for what concerns particular and judicial data and processing operations, executable in fulfillment of an access request. The activities aimed at applying this regulation are considered to be of significant public interest.

When the processing concerns data revealing the state of health or sex life, processing is allowed, if the legally relevant situation that is intended to protect with the request for access to administrative documents is at least equal to the rights of the data Subject, i.e., it consists of a personality right or another fundamental or inviolable right or freedom.

As regards restrictions to generalized civic access deriving from the protection of personal data, please see the ANAC guidelines No. 1309/2016.

5. MANAGEMENT OF FACILITIES AND PHYSICAL RESOURCES

All FBK premises and all physical resources must be used and stored with the utmost diligence in order to guarantee an efficient working activity and an adequate level of information security by following these Regulations to ensure the physical safety of FBK areas and assets.

6. ACCESS TO RESTRICTED OFFICES AND AREAS

Premises and offices. Access to offices, protected areas, and areas reserved to paper archives is allowed to authorized Users with a personal badge, based on precise and motivated work requirements.

The data relating to the transits tracked by the personal badge may be made available to the Heads of the aforesaid offices, areas and archives for purposes of security and property protection.

Further and specific access to offices and protected areas may be granted and enabled by the Safety and Protection Unit only upon a written request including reasons from the various respective Heads.

Visitors and guests may access the above-mentioned FBK areas only upon registration at check-in, showing the pass received at registration and if accompanied by an Internal User.

Data Center. Access to the FBK Data Center premises is permitted only to authorized personnel through biometric system or personal badge.

Exceptionally and for a short periods, visitors and guests can be granted access to the Data Center, provided they are authorized and accompanied by authorized FBK personnel. Visitors and guests must be adequately instructed by authorized personnel regarding the characteristics of the environment, the existing risks, the good practice standards provided for and the procedures to be implemented to prevent or manage emergencies and risks.

For safety reasons and to keep the operating temperature constant, all access gates must remain open only for the time strictly necessary for the passage of people and materials.

For security reasons, a picture is taken to anyone accessing the FBK Data Center and this image is immediately sent to authorized personnel in charge of the Data Center.

The above rules also apply to the Disaster Recovery site.

7. CORRECT USE OF BADGE

The personal badge is issued by the Safety and Prevention Unit once the data entry procedure has been completed. The technical processing time for preparing the badge is on average 5 working days. The badge is considered a strictly personal object; it must therefore be properly kept and cannot be lent, not even temporarily.

In case of unauthorized use, the badge will be immediately withdrawn by the surveillance personnel and sanctions may be applied.

The loss of the badge should be immediately reported to the Safety and Prevention Unit, which will deactivate it. In case of replacement, the new badge will be issued by the Safety and Prevention Unit at the User's expense.

Upon termination of the employment relationship with FBK, the badge must be returned to the Safety and Prevention Unit.

8. VIDEO/AUDIO RECORDINGS AND PHOTOGRAPHS AT FBK PREMISES

All video/audio recordings and photographs must respect the rights of the individuals involved.

Internal Users: for reasons connected to their work activity, video/audio recordings and photographs must be authorized by the User's Supervisor. They must be used exclusively for work purposes and cannot be disclosed outside the institutional context in which they were created.

Any other video/audio recordings and photographs of any area of FBK are forbidden, with the exception of those previously and formally authorized by the User's supervisor after having consulted with the Digital Communication and Big Events Unit.

Internal Users can be photographed and/or recorded at events, seminars and training sessions as well as for the documenting of institutional activities, especially research-related ones. In these cases, images and footings may be used for institutional purposes and communications.

To strengthen internal security in an organizational context in which the Foundation's premises are accessible to third parties, personal profile pictures must comply with certain standards and their publication is, by default, mandatory on the Foundation's internal networks.

External Users: Making video/audio recordings or taking photographs in any area of FBK is prohibited. Any exceptions must be authorized by the Digital Communication and Big Events Unit. The Internal User acting as the contact of an External User is required to enforce these provisions.

9. WORKING STATIONS

The use of the workstation and the consequent access to documents, deeds and archives is permitted within the limits of the User's function and duties.

Clean desk. Users must keep their desks clear, and make sure they do not leave confidential documents and deeds without controlling third parties from accessing them during breaks, at the end of the workday and/or during any time off.

10. PHYSICAL MEASURES TO SAFEGUARD PAPER DOCUMENTS AND RECORDS

Paper data and paper records necessary to carry out work tasks must be kept in storage cabinets or drawers in the working context in which the User operates. Access to all archives is restricted, thus Users are allowed to

access them only when needed and only to take out and put back the documents needed to carry out their tasks. The documents should be put away properly in the storage cabinets when the User steps away from the office and at the end of the working day.

Archives containing particular (former sensitive) documents and records must be kept in locked storage cabinets.

The physical elimination of any paper document or ICT support containing company and/or personal data and information must only be carried out using the appropriate tools.

It is recommended not to leave documents unattended at the printing devices.

11. MANAGEMENT OF PERSONAL AND CORPORATE DATA

Each User is responsible for the data and information that he/she enters into possession when performing his/her work. It must therefore process data and information by adopting all appropriate security measures in order to protect its confidentiality, security, integrity and correct use.

The data and information may be communicated to third parties exclusively within the scope of the User's function and according to the purposes related to his/her work.

The disclosure of data and information to third parties that may damage the image, reputation, productivity, intellectual property as well as the know-how and profitability of the Foundation or that may violate the contractual and legal obligations related to the work relationship is forbidden.

The disclosure to third parties of confidential, classified or otherwise proprietary information of the Controller is strictly prohibited. In case of breach, the Controller reserves the right to initiate the related disciplinary sanctions, as well as the civil and penal actions allowed.

Users should also be reminded that the illegal dissemination of data and information could, in addition to the violation of these Regulations, result in the violation of rules with both civil and criminal consequences against the perpetrator of illegal activity, as well as violation of the regulations governing the work relationship.

12. ICT SYSTEMS

The ICT systems supplied should be used for professional purposes. Notwithstanding this principle, FBK authorizes a moderate and reasonable private use. This use must be limited and based on criteria of common sense and must not hinder professional use. Space in the entrusted instrument used for "private" purposes (for example the dislocation of data, photos or video files), must therefore be limited and must not preclude and limit the one dedicated to professional use.

All tools must be locked and password protected if left unattended.

The instruments must be automatically turned off or put into low-power mode if not used for more than an hour, unless otherwise required by research needs.

FBK provides Users with different types of networks:

a. Internal, reserved to centrally managed FBK-owned IT devices;

b. External, reserved to privately-owned or non centrally managed IT devices;

c. DMZ, reserved to centrally managed servers offering services to non-FBK Users.

System Administrators only have access to managed IT systems connected to the FBK internal and DMZ networks with Administrator or "root" privileges, both local and network. During certain periods in which a User

moves away from FBK, it is possible to raise the User's local privileges on his/her supplied portable workstation. The device on which the access privileges are modified must be, without exception, initialized and reinstalled upon return.

On FBK internal networks and centrally managed devices, it is not permitted to modify in any way the operating system or the applications installed by the System Administrators that comply with the appropriate security measures.

Furthermore, FBK has signed a specific agreement with the Consortium of the Italian Network of Universities and Research, which manages a network commonly known as the "GARR Network". The use of IT devices is User to compliance with the *Acceptable Use Policy* of the GARR network available at the following link*:* https://www.garr.it/it/regole-di-utilizzo-della-rete-aup.

13. POSSIBILITY OF INDEPENDENT MANAGEMENT OF FBK-OWNED DEVICES

To the end of ensuring maximum flexibility to research, Internal Users working for the Research Divisions only may, upon authorization of their immediate Supervisor and of the System Administrator, obtain the full delegation to the management of FBK-owned ICT devices for the sole purpose of conducting research activities. The instruments configured in this way cannot be connected to FBK internal and DMZ networks, but must be used on external networks.

When choosing this particular mode of use, the User accepts to be appointed as "FBK-owned ICT tools Administrator". This figure must provide assurance that he/she can implement technical measures and organizational arrangements in such a way that the processing meets the requirements of the GDPR and ensure the protection of the rights of the data Subject and of the data of which FBK is the Data Controller. Such authorized Users must attend preliminary and periodic training, as required by the laws in force, with the final aim of providing basic concepts concerning the appropriate security measures and the general obligations envisaged by the legislation on Privacy in force.

The following are the rules for using the aforementioned self-managed IT tools:

- Access to the Internet will follow the same rules as those for the Eduroam network.
- The internal FBK network will accessible through SSL VPN and will comply with the same rules in force for personal instruments.
- IT devices will be visible among them without port or protocol restrictions.
- IT devices will not be allowed to offer neither direct nor indirect services to the Internet.
- IT tools will be accessible from the internal network directly and from the outside, for maintenance reasons, only through SSL VPN.
- IT tools should not interfere with the normal functioning of the network.
- Independent management implies the ability to manage and debug IT tools. The installation of the operating system will be carried out by the User. Backup services are not provided. Windows licenses will be charged to FBK, while the Linux licenses will be charged to the User.
- The support of the IT, Infrastructures and Corporate Assets will be limited to the hardware part only as provided by the warranty. No support with software issues will be provided.
- The instructions for connecting the systems to the networks and the debug methods for connecting to the network can be found at the IT, Infrastructures and Corporate Assets Service website.

- In the event that multiple Users share the IT device, the Unit Head will act as the User in charge of the independent management.

The same procedure shall be followed also by those internal Users who use FBK-owned smartphones or tablets.

14. CARE OF ICT TOOLS

Users should take good care of FBK-owned IT tools, avoiding any damage that could hinder their proper functioning and avoiding leaving them unattended in public areas.

In case of theft or damage of goods, the User must immediately notify the IT, Infrastructure and Corporate Assets Service, submit a formal complaint to the public security authorities and deliver a copy to the above mentioned Service for the activation of the formal procedures of update of assignment to user information and insurance coverage.

15. DATA MANAGEMENT AND PROTECTION

The authentication credentials for access to the network and to other services are provided by the IT, Infrastructures and Corporate assets Service, and delivered to the User by the Safety and Prevention Unit. They can be modified by the User and consist of a code identifying the User (username), associated with a reserved password that must be protected by the User with the utmost diligence and not be disclosed. Each User is responsible for security and for any operation performed using his/her credentials. Accessing the network and programs with credentials other than their own or anonymously is prohibited.

In case of need to renew the credentials at the end of the employment relationship, the related requests must be granted only if in connection with an affiliation relationship.

In order to maintain an active relationship with those who have contributed with their vision to achieving its strategic objectives, the Foundation accepts the possibility, subject to authorization from the Secretary General, that the personnel who have held a position of responsibility may maintain access to Google services and Microsoft transforming the e-mail domain into @exstaff-fbk.eu.

16. DATA MANAGEMENT AND PROTECTION

Access to data is permitted within the limits of one's organizational function and work activity.

The network discs present on FBK's servers are sharing areas for strictly professional information and cannot in any way be used for different purposes. Therefore any files that are not inherent to the work activity cannot be stored, even for short periods, in these units. Regular checks, administration and backup activities are performed on these units by authorized staff.

Please note that no backup will be performed on discs or other local storage units by the authorized staff. Saving the data contained in such units is therefore the individual User's responsibility.

Authorized staff may at any time proceed with the removal of any file or application that they consider dangerous for security both on the ICT tools of Users and on the network units: the User and his/her immediate Supervisor will be informed of this action.

Backups of the main network servers are performed by the System Administrators, who retain them for five years. Users who retain FBK data in areas for which backup is not provided are responsible for saving them and for any damage to FBK or third parties, including those of a civil nature caused by their loss or subtraction.

Users should be aware that, without prejudice to the existing obligations to protect its employees' privacy, the data processed by them on FBK's IT systems may be owned by FBK or otherwise under the responsibility of FBK. In order to guarantee the security and integrity of the information present on FBK's IT systems, the confidentiality of the information in case of inspections cannot be absolutely guaranteed.

Temporary storage of data on private ICT tools is permitted provided that the aforementioned instruments are protected so as not to allow access by unauthorized external Users.

Saving corporate data and information in public cloud systems that are not authorized by the System Administrators is prohibited.

Team Drive, part of the Google G-Suite storage cloud, should be used as an alternative to the network disks on FBK servers. For this service apply all criteria for network disks on FBK servers without prejudice to data backup for which G-Suite terms apply.

Since the Foundation interacts with Public Administrations, when developing software, applications and codes that process personal data, it is necessary to respect and adopt the guidelines provided by the Agency for Digital Italy (AGID) on ICT security precautions, following development methodologies that take into account privacy and cybersecurity issues.

17. MANAGEMENT OF ELECTRONIC MAIL

FBK grants e-mail accounts (hereinafter "FBK e-mail") to its staff for professional us. Notwithstanding this principle, FBK authorizes a moderate and reasonable private use. This use must be limited and based on criteria of common sense and must not hinder professional use. The space used for "private" purposes must therefore be limited and must not preclude and limit that dedicated to professional use.

The Foundation, in compliance with the regulations on privacy, provides that each outgoing message be automatically added a short text warning the recipient of the potentially confidential nature of the message.

FBK e-mail account holders are responsible for its use and must make use of e-mail in an acceptable manner.

In particular, Users must comply with the following provisions:

- Do not send or store emails and/or attachments with offensive, harassing, vulgar, blasphemous, xenophobic, racial, pornographic or otherwise inappropriate or illegal content, unless specific research needs require so;
- Pay the utmost attention when sending e-mails containing personal data, which should be adequate, relevant, and limited to what is strictly necessary for the purposes for which they are sent;
- Pay the utmost attention when forwarding e-mails containing contents and e-mail addresses of previous communications;
- Pay the utmost attention to suspicious e-mails, and report them to the System Administrator in case of concerns about their origin/content;
- create a section called "Personal Mail" in your inbox, which the System Administrators will not be permitted to access except for serious information security reasons.

For cybersecurity reasons, and in case of sudden or extended absence and urgent work-related needs, access to the User's mailbox may be managed by the System Administrators at the request of the User's Data Protection Manager to verify the content of the messages and to forward to the Data Controller those deemed relevant for performing the work activity.

Certified Electronic Mail (Posta Elettronica Certificata, PEC) may be used by employees in charge/authorized staff for professional purposes only.

18. INTERNET BROWSING

Internet access is provided primarily for professional purposes, to access information and content necessary for conducting work activities. Being a work tool, the Users who are given access to it are responsible for its correct use. As for e-mail, FBK authorizes a moderate and reasonable private use, limited and based on criteria of common sense without obstacles to professional activity.

Please be informed that the number and duration of Internet browsing activities are constantly recorded. The consultation of these recordings can only take place anonymously and in aggregate except in the cases provided for by law and failure to comply with these Regulations. Any checks by the System Administrators may be carried out by means of a system for analyzing log files. Users must abide by the following Internet browsing rules:

a. it is strictly forbidden to download material and programs in violation of copyright law, whether they belong to people or companies, covered by copyright, patent or intellectual property, including the installation or distribution of software that is not specifically licensed for use within FBK;
b. it is strictly forbidden to browse sites and to download dangerous/forbidden or illegal contents (offensive, harassing, vulgar, blasphemous, xenophobic, racial, pornographic, child pornography, terrorism or otherwise inappropriate or illegal content), except for specific research needs;
c. it is forbidden to make unauthorized copies of copyrighted material including but not limited to digitizing and distributing photos from magazines, books or other sources, music or video material;
d. it is forbidden to use the technological infrastructure of FBK to procure and disseminate material in violation of the current regulations;
e. it is forbidden to carry out activities that may generate security problems or damage communications on the network;
f. it is forbidden to conduct any form of monitoring of the network that allows to capture data not expressly sent to the user host (sniffing) unless this activity is part of the user's duties and therefore formally authorized by the system administrators;

It is forbidden to bypass the authentication procedures or the security of any host, network, account.

19. INTERNET ACCESS FOR NON-FBK USERS

A system to allow access and Internet browsing to external Users is in place.

The number and duration of Internet browsing activities are constantly recorded.

20. REMOTE ACCESS - VIRTUAL PRIVATE NETWORK (VPN)

Access from outside the FBK network is only permitted through specific secure connection methods, indicated on the IT, Infrastructures and Corporate Assets website. Any other access method is strictly forbidden.

21. USE OF HIGH PERFORMANCE COMPUTING (HPC) SYSTEMS

The additional rules for the use of High Performance Computing systems are covered in Annex A.

22. COMMUNICATION OF DATA AND INFORMATION THROUGH SOCIAL MEDIA

Publishing on the Internet through personal social media, forums, chats, blogs, websites, professional data and information (information, documents, notes, personal or third-party comments, photos, videos, audio, etc.) that may damage the image, reputation, productivity, intellectual property and know-how and profitability of FBK, or that may violate the contractual and legal obligations associated with the User's employment relationship with the Foundation is strictly forbidden.

The dissemination of false information is strictly forbidden.

However, the disclosure of information already made public by FBK is authorized; in case of any concerns, the Digital Communication and Big Events Unit should be consulted.

23. MONITORING SYSTEM OF THE FOUNDATION'S NETWORK

Due to computer system security, technical and/or maintenance reasons (for e.g., update/ replacement/implementation of programs, hardware maintenance, etc.), or for the purposes of controlling and programming costs (e.g. verification of connection to the Internet, telephone traffic, etc.), even if unrelated to any purposes of working activity monitoring, it is the Data Controller's right, through the System Administrators and in compliance with privacy regulations, to access directly all FBK's IT tools.

Periodically, and in the event of anomalies, System Administrators will carry out in-depth functional checks that will determine generalized notifications and warnings to the Users of the organizational function in which the anomaly has been detected and will invite the parties concerned to scrupulously follow the assigned tasks and the instructions given.

Checks on an individual basis may be performed only in case of further anomalies.

System Administrators also carry out non-personal network checks and on all the devices that compose it. Details of the checks carried out are available in Appendix B.

In no case will prolonged, constant or indiscriminate inspections be performed.

However, FBK is obliged to report to the judicial authorities all illegal actions, including those detected by non-personal inspections.

24. DIGITAL SIGNATURE USAGE

The Digital Signature must be used exclusively by the owner of the signature.

25. VIDEOSUVEILLANCE SYSTEM

The video surveillance system is implemented in some specific areas (appropriately indicated by information signs) for security and check purposes to protect the assets of FBK against vandalism, unauthorized access or technical and structural failures, illicit and/or fraudulent behavior and to facilitate operators in checking structure safety.

Access to the videotaped images is permitted, exclusively for the above purposes, to the persons in charge of processing/authorized staff and, in case of necessity, to the law enforcement agencies.

The document on Video Surveillance is adopted by the Video Surveillance Chief Officer appointed by the Board of Directors and updated as needed.

26. SPECIFIC PROHIBITIONS

The specific prohibitions for Users are as follows:

a. altering IT documents, public or private, having evidential value;

b. illegally accessing the IT or telecommunications system of public or private Users;

c. illegally accessing one's own computer or telecommunications system in order to alter and/or delete data and/or information;

d. illegally keeping and misusing codes, keywords or other means suitable for access to one's computer or telecommunications system or those of competitors, public or private, in order to acquire confidential information;

e. carrying out activities of procurement and/or production and/or deployment of equipment and/or software in order to damage an IT or electronic system of public or private Users, the information, data or programs contained therein, or to favor its total or partial disruption, or the alteration of its operation;

f. carrying out fraudulent activities intended to intercept, prevent or disrupt communications;

g. editing and/or cancelling data, information or programs of private Users or public entities or in any case of public benefit;

h. carrying out activities that damage information, data and computer programs or other people's programs;

i. destroying, damaging, making IT or telecommunications systems of public benefit unusable;

j. uploading programs not originating from a source that is reliable and has been authorized by the Company;

k. purchasing software licenses from a source (retailer or other) that is not certified and cannot guarantee the originality/authenticity of the software;

l. owning storage media for non-original programs (DVD\CD\floppy discs);

m. installing a number of copies of each licensed program higher than the copies authorized by the license itself, in order to avoid falling into possible underlicensing situations;

n. illegally using computer passwords, access codes or similar information to perform any of the above-mentioned actions;

o. using tools or equipment, including computer programs, to decrypt software or other IT data;

p. distributing FBK-owned software to third parties;

q. creating software code that infringes third party copyrights;

r. illegally accessing and duplicating databases.

27. REVOCATION OF AUTHORIZED DATA PROCESSOR STATUS

In case of revocation of the status of data processor or termination of the employment relationship with FBK, the following operating rules apply:

a. Credentials for system and e-mail access are disabled.

b. FBK has the right to retain any professional e-mail of Users no longer belonging to the organization. E-mails in the "Personal Mail" folder will, on the contrary, be deleted.

These activities are performed by System Administrators authorized to manage e-mail accounts, who may therefore have access, for exclusive technical reasons and only where it is not avoidable, to personal data stored in e-mail accounts.

Internal Users are required to set up, with due advance, the auto responder to notify any suppliers, partners, customers or other interested parties, about the interruption of their work relationship with FBK and - if applicable - to propose an alternative internal contact.

With regard to returning FBK-owned ICT tools, the following operating rules apply:

a. Smartphones and tablets must be returned to the IT, Infrastructure and Corporate Assets Service.

b. Other ICT tools entrusted to Users of the Research Centers must be returned to the Head of the Research Unit they worked in.

c. ICT tools entrusted to Users of the Administration Departments will be returned to the IT, Infrastructure and Corporate Assets Service.

28. PERSONAL DATA BREACH

"Data breach" means the security breach that involves unintentionally or unlawfully the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

All cases of personal data related violations must immediately be reported to the Data Protection Officer (privacy@fbk.eu) thus ensuring the activation of the procedure for handling security breaches.

29. FURTHER PRESCRIPTION

For doubts and concerns regarding acceptable practices for the processing of personal and business data and information, as well as the use the processing tools, Users can contact their Supervisors and the Prevention of Corruption, Transparency and Privacy Unit to receive the appropriate instructions.

30. LIABILITY AND SANCTIONS

All Users are required to comply with the provisions made known through these Regulations. Users who fail to comply with or breach these Rules can be prosecuted with disciplinary and compensatory measures provided for by the current FBK Disciplinary Code, as well as with all civil and criminal actions provided by the law.

Anyone who does not comply with these Regulations may be immediately revoked access to ICT tools.

31. UPDATE AND REVISION

These Regulations are reviewed periodically, either as a result of organizational and regulatory changes or institutional needs. All future amendments to these Rules will be communicated and published on the FBK website.

Read and approved on January 29, 2019

- Prof. Francesco Profumo -

President of Fondazione Bruno Kessler

Addendum A

Additional rules for the use of High Performance Computing Systems

I – High Performance Computing Systems (hereinafter "HPC) Users

1. All operating research units may use HPC systems by requesting access or support to help-it@fbk.eu.
2. The Heads of the Research Operating Units using HCP systems will participate in a board called "Cluster-Strategic". This board will make strategic decisions concerning the HPC Systems.
3. The Heads of the Research Operating Units using HCP systems will elect one or more members of a second board called "Cluster-Technical". This board will make technical decisions about HPC Systems.
4. All other requests should be submitted to Cluster-Strategic (cluster-strategic@fbk.eu).

II – Use of HPC Systems

1. Users must use Secure Shell (SSH) tools to login into HPC Systems and Secure Copy Protocol (SCP) to transfer files from and into HPC Systems. The systems will not accept incoming connections from any other protocols. For security reasons, once users are logged in, outgoing connections will not be allowed.
2. The machines accepting SHH connections, called "Logon Servers", will act as front-ends. They may be used for editing, compiling/debugging of small applications and for preparation and submission of batch executions.
3. The execution of programs using extensively the CPU of Logon Servers is not permitted. These types of executables (targz, compile and debug sessions, etc.), must be run 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 types 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. Users are strongly encouraged 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. The system will alert Users when a job has been:
   a. killed (with reason);

   b. suspended (with reason);
   c. resumed;
   d. running for a long time.
2. Users may configure the system so that it will also alert them for:
   a. Job started;
   b. Job accomplished.

Addendum B

Details relating to check activities carried out by System Administrators

FBK 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

Electronic mail account- Stored data:

1. log of SMTP traffic generated by the e-mail server;
2. log of messages not forwarded correctly (delays and/or non-delivered);
3. log of messages intercepted by the antispam system;

IP traffic – proper functioning of the system, SLA monitoring, security checks:

a. log of http/https traffic generated on IT 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).

Access to networks - proper functioning of the system, SLA monitoring, security checks:

a. Log of internal and external access to networks.

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