ISTITUTO ITALIANO DI TECNOLOGIA

Procedure for the correct use of ICT resources

Revision	Amendment Description	Author	Approval	Date
01	First version	ICT	D.S. D.G.	23/02/2022

CONTENTS

1. AIMS AND PURPOSES

The aim of this document is to define the detailed procedures for correct use of the ICT Resources provided by the IIT Foundation (hereinafter, also the "Foundation" or "IIT") to its Users (as better defined in 2.2) for the performance of their work duties, with the following purposes:

- to fulfil the obligations established by current national legislation on the protection of personal data (GDPR), the Workers' Statute (art. 4 paragraphs 2 and 3 of Law no. 300 of 20 May 1970) and the "Guidelines of the Data Protection Authority for the protection of personal data for e-mail and Internet of 10 March 2007";

- to train, inform and make Users aware of the permitted uses of the ICT resources received;

- to define the controls permitted to the Data Controller regarding personal information detectable from the use of ICT Resources provided to Users.

The recipients of this Procedure are therefore all IIT Users.

2. INTRODUCTION AND DEFINITIONS

2.1. Introduction

The ICT Resources of the Foundation constitute one of the strengths of the latter and it is therefore necessary to guarantee their development and management based on principles of effectiveness and efficiency; at the same time, they can be a source of risk for the security of the information being handled and for the image and reputation of the Foundation.

For this reason, IIT provides its Users with diversified work tools according to the role of each and on the basis of their professional requirements, and all Users must be informed and accept the principles on the subject of permitted use, as formulated in this document and in accordance with the Foundation's Code of Conduct and Scientific Conduct.

.

2.2. Definitions

Name:	Abbreviation	Description
User		Anyone who has an employment or collaboration relationship (including temporary staff, apprentices, interns), and external personnel affiliated with the IIT Foundation who carry out scientific, professional or study research activities within the IIT facilities.
Personal Data	P.D.	Any information relating to a natural person, identified or identifiable, even indirectly, by reference to any other information, including a personal identification number.

Name:	Abbreviation	Description
System Administrator	AdS	Professional position aimed at the management and maintenance of a processing system or of its components. In the IT field, other comparable figures are also considered as such from the point of view of risks relating to data protection, such as database administrators, network and security equipment administrators and complex software system administrators.
Security incident		An event that compromises or could compromise the confidentiality, integrity or availability of the information system or information being processed, or that represents a breach or an immediate threat of breach of the security policies defined by the Foundation.
ICT Contact		The employee/collaborator of the Data Controller with particular tasks in the management and maintenance of business applications and of the technological infrastructure of the peripheral structures of the Data Controller.
ICT Resources	R.I.	Equipment and applications (HW/SW) that allow access to and/or the creation, recording, display, reproduction and/or transmission, electronically, of data and documents.
Data Controller		The natural person, the legal person, the public administration and any other body, association or organisation which is responsible, even jointly with another Data Controller, for decisions regarding the purposes, methods of processing of personal data and the tools used, including the security profile.
Breach of personal data		A breach of security that results in the destruction, loss, alteration or the unauthorised or unlawful disclosure of personal data transmitted, stored or otherwise processed (GDPR, art. 4(12)).

3. DOCUMENTS AND TOOLS

Type	Name:	Use	Link
Policy	Code of Conduct and of Scientific Conduct	It defines the general principles and guidelines that must inspire the behaviour of all those subjects who in various capacities interact with the Foundation	https://intranet.iit.it/modello-organizzativo-231/1121-codice-di-comportamento-rev-07-eng/file
Policy	ICT Policy	It establishes the correct use of IT systems in the IIT Foundation, protecting IIT and Users from the risk of compromising the IT systems, from undue disclosure of personal and confidential data, and from the related legal consequences, also making the use of IT systems more effective	https://intranet.iit.it/policies/policies-guidelines-eng/1133-po-11-policy-ict-rev06-en2/file
Policy	Information Security Policy	It defines the rules for safe use of the IIT Foundation information system, including the classification of information	https://intranet.iit.it/policies/policies-guidelines-eng/1135-p-26-policy-informationsecurity-eng/file
Policy	Acceptable Use Policy – GARR Network	It defines the rules of use of the GARR Network	https://www.garr.it/en/acceptable-use-policies
Register	Data controller's register	Foundation's processing register	https://intranet.iit.it/offices/legal-affairs/privacy/privacy-organization/adempimenti-gdpr-semestrali-iit/723-registro-dei-trattamenti-iit-titolare/file
Procedure	Management of Data Breaches	It governs the Data Breach management process, in accordance with the provisions of art. 33 and 34 of the European Regulation 679/2016	https://intranet.iit.it/offices/legal-affairs/legal-procedure/1978-io-lo-03-gestione-data-breach-eng/file

Type	Name:	Use	Link
Policy	Code of Conduct and of Scientific Conduct	It defines the general principles and guidelines that must inspire the behaviour of all those subjects who in various capacities interact with the Foundation	https://intranet.iit.it/modello-organizzativo-231/1121-codice-di-comportamento-rev-07-eng/file
Procedure	Appointment and control of system administrators and super users	It defines the methods for the periodic collection of names of System Administrators and of Super Users and the verification activities to be carried out in order to ensure compliance of their work with the relevant legal provisions	https://intranet.iit.it/offices/legal-affairs/legal-office/legal-procedures/2715-io-lo-11-amministratori-di-sistema-e-superusers-eng/file
Procedure	Access to data in case of sudden or extended absence	It defines and regulates the methods of access to company data managed by Users within the Foundation's ICT systems, in cases of sudden or prolonged absence of the User during which urgent needs related to work or from which prejudicial consequences for the Foundation may arise occur	https://intranet.iit.it/offices/information-and-communication-technology/ict-procedures/ict-procedures-1/599-io-it-04-access-procedure-to-data-pubblicata/file
Procedure	Logical accesses procedure	It establishes rules for the creation, management, assignment and removal of privileges and users in the ICT systems of the Foundation in order to ensure that security measures are met to mitigate possible risks relating to the Confidentiality, Integrity and Availability of information and ICT systems	https://intranet.iit.it/offices/information-and-communication-technology/ict-procedures/ict-procedures-1/601-io-it-05-logicalaccess/file
Procedure	Procedure for the Management of ICT Security Incidents and Logs	It defines the management of logs and the management of ICT incidents, with particular attention to ICT Security incidents, including an escalation procedure for reporting illegal or presumed illegal activities to the judicial authority and/or postal police	https://intranet.iit.it/offices/information-and-communication-technology/ict-procedures/2278-io-it-07-gestione-incidenti-sicurezza-e-log/file

Type	Name:	Use	Link
Policy	Code of Conduct and of Scientific Conduct	It defines the general principles and guidelines that must inspire the behaviour of all those subjects who in various capacities interact with the Foundation	https://intranet.iit.it/modello-organizzativo-231/1121-codice-di-comportamento-rev-07-eng/file
Procedure	ICT procedure for the assignment of mobile telephony devices	It defines the operating procedures for requesting the assignment of telephone and data transmission equipment on mobile networks and related telephone cards	https://intranet.iit.it/offices/information-and-communication-technology/ict-procedures/603-io-it-02-procedura-ict-per-lassegnazione-degli-apparati-di-telefonia-mobile-v2/file

4. DESCRIPTION

The rules set out below are intended to protect IIT and Users from the risk of compromise of the ICT systems, from the undue disclosure by of P.D. and of confidential data, and from the related legal consequences, as well as to make the use of ICT systems more effective. In the following provisions, reference will also be made to a number of definitions provided for by the current legislation applicable to the protection of P.D.

4.1. Responsibility of Users

In compliance with the current ICT Policy (quoted, prf. 3.4), the main responsibilities of Users on the correct processing of information in accordance with the principles defined in this document are briefly recalled here:

- they must operate exclusively within the scope of the role assigned, of the work activities required of them, of the assignment received and of the systems they have been authorised to use;

- they must be aware of their responsibilities regarding information security and relevant to their work duties, ensuring, for example, an adequate level of participation in initiatives of training and of awareness-raising on security and of knowledge of data classification policies;

- they must guarantee that IIT data are never kept in single copy on devices assigned to the EndUser and in any case that they are kept on such devices only for the time strictly necessary, and that a main copy is always available in the workspaces dedicated to this purpose;

- they must not disclose any private, confidential or secret information to unauthorised individuals or entities without adequate authorisation and must avoid the inadvertent disclosure of confidential information in compliance with IIT's Information Security Policy;

- they must promptly inform the ICT Management, by contacting the appropriate referents according to the procedures in force, regarding:

- possible cyber incidents;
- possible breaches of P.D., in which case reference should be made to the "Management of Data Breaches" procedure which requires immediate reporting to the Legal Affairs Department;
- possible breaches of security policies or possible improper use or use different from the requirements formulated in this document;
- the loss or theft of R.I. owned by IIT or containing information owned by IIT;
- a suspected or confirmed breach of the User's access credentials, for example in the event of observation of activities carried out on behalf of the User of which they are not aware;
- unusual behaviour of R.I. assigned to users or the receiving of security warnings, such as malware that apparently cannot be removed/eliminated/repaired, the receiving of anomalous amounts of pop-ups or content that automatically starts downloads;
- the receiving of excessive amounts of unsolicited e-mails (spam), e-mails with illegal or harassing content, or presumably containing malicious links.

In case of uncertainty, the User must promptly report to the ICT Management staff the improper use (suspected or actual) of any R.I., with opening of a ticket with the ICT Service Desk (e-mail: ICT_ServiceDesk@iit.it).

Any non-fulfilment of these responsibilities, incorrect use of R.I. and abuse of the related policies and procedures may be reported for possible measures to be taken in accordance with the terms of the contract and the relationship between the User and the IIT Foundation, the Foundation's Code of Conduct and the Code of Scientific Conduct, and in accordance with the ICT Policy (quoted, prf. 3.6), according to the principles of proportionality and graduality.

4.2. Permitted controls

In order to ensure the appropriate use and correct maintenance of the R.I. and to manage any security incidents or breaches of P.D., in accordance with the applicable mandatory legislation and with the permitted activities defined in the ICT policy (quoted, prf. 3.5), the ICT Management through its AdS can carry out checks and verifications (using specific tools) at the physical and logical access points to the ICT infrastructures and applications, as indicated by the processings of the ICT Directorate listed in the appropriate IIT register, available for consultation on the Intranet.

These processings define the means and purposes of the same, the data collected with the relative retention periods, as well as the list of AdS appointed to carry out the individual processings, and specifically concern:

- management of the R.I. assigned to the User throughout their entire life cycle, carried out through asset and software registration tools also used for the installation of application updates;
- management of the security measures set on the R.I. assigned to the User, activated through antivirus/antimalware and threat detection tools, personal firewalls, device encryption, and tools for verifying their compliance with the configurations adopted, such as, but not limited to, Endpoint Detection and Response and Mobile Device Management solutions;
- management of logs of access to the network and to network tools, such as, by way of example but not limited to, solutions of Internet browsing, mail, and the cloud platforms of Microsoft Teams, Sharepoint and OneDrive.

The technologies used comply with the requirements of the applicable laws in force and are limited in access to authorised personnel only, as prescribed and permitted by law.

It should be noted that IIT does not carry out checks on logs for control purposes towards Users, but only in order to safeguard the security and performance of its systems, as well as to guarantee the correctness and appropriateness of the data and the management of information relating to general expenses and in particular, not in a limiting way, in order to prevent or counter breaches of the confidentiality of other Users or third parties, changes to ICT systems and information transmitted, cyber attacks (such as the presence of viruses or other malware), hacking, the use of Internet access

or other unapproved network access systems, or behaviour differing from the "Acceptable Use Policy" of the GARR network.

These checks can take place at any time and also on a periodic basis, or with sample tests, in relation to internal controls, civil proceedings, government investigations or assessments, and to other legal and regulatory proceedings: in any case, as already indicated above, the data recorded for this purpose will in no way be used to remotely control the Users' activities. In this regard, it is also specified that in the event of checks, in compliance with the principle of "data minimisation", they are carried out gradually, favouring a preliminary check on aggregate data, referring to the entire organisation or its areas, which may end with a generalised notice relating to a detected anomalous use of company tools and an invitation to strictly comply with the tasks assigned and instructions given. In any case, the carrying out of prolonged, constant or indiscriminate verifications is excluded. If necessary, based on the outcome of the verifications, AdS can proceed to the timely removal of any file or application considered dangerous for security, both on workstations and on network drives.

4.2.1. Emergency accesses

Users must also be aware that, in full compliance with current legislation and protecting the principles of privacy, R.I. can be withdrawn at any time in order to verify the data contained therein for operational, legal or security reasons, such as for example to comply with legal or regulatory requirements, in the context of an internal investigation or similar investigations, or in the event of an unexpected or prolonged absence of a User, in line with the procedure "Access to data in case of sudden or extended absence". In accordance with the ICT policy (quoted, prf. 3.3) and in compliance with the laws regarding the protection of P.D., the assignee of the R.I. subject to the assessment will be adequately informed about the possible processing of the data resulting from the verification and control activity.

5. RULES FOR THE CORRECT USE OF ICT RESOURCES

The following paragraphs explain the rules relating to the appropriate use of R.I.s provided to Users, together with the limits according to which said R.I. can be used to manage the information life cycle, divided into the three families listed below: "Authorisation and Access", "End-point", "Network tools".

5.1.Authorisation and access

5.1.1. Management of personal accounts and authentication credentials

All access or connections to R.I. must be formally authorised and take place through credentials that allow user authentication and to consequently regulate access to R.I..

These credentials must therefore be nominal, that is, uniquely associated with the assignee through a user account, and protected through the use of a code known only to the User (normally, a password).

Each User is therefore responsible for the use of their own credentials and in particular MUST:

[R1] change the password communicated during the initialisation phase of their account at the first access to the supplied PC;

[R2] keep their authentication credentials (which constitute P.D.) strictly confidential without communicating them or sharing them with third parties, not even at the request of the ICT Service Desk or own manager;

[R3] immediately report to the ICT Service Desk if they suspect that their authentication credentials have been identified by someone or used in an unauthorised manner, following the instructions received for changing the password and applying the procedure "Management of Data Breaches" on the breach of P.D.

Similarly, the User MUST NOT:

[R4] write down their password on paper (post-it type) or in cleartext electronically (for example via e-mail).

In the event that breaches of security policies are detected through a given account, IIT can deactivate it remotely upon short or even no notice, also in order to prevent cyber attacks that could be perpetrated through this account.

In case of interruption of the employment relationship with the User, the above authentication credentials will be disabled within the day following the end of the collaboration; however, final and total deletion of the user account will take place within 6 months.

Regarding the password management policy, i.e. the criteria for its construction and its duration, reference is made to the provisions of the "Logical Accesses Procedure".

5.1.2. Privileged account management

As most cyber attacks exploit elevation of privilege, the use of so-called "privileged" accounts (i.e., those accounts that have higher access rights for local administration of the R.I. assigned to the User) is governed by application of the "principle of least privilege", by defaulting to each User a non-privileged profile on the assigned computer. Any requests for privileged profiles must follow the "Logical Accesses Procedure".

In any case, given their intrinsic nature of greater risk, privileged accounts can be monitored to verify potential unauthorised access during their use, to the extent that this is permitted and required by the laws in force on the protection of P.D.

5.1.3. Network access

Each User may access the IIT network through the R.I. assigned to them through the wired connection or through the Wi-Fi connection, using their own credentials.

Connection to the IIT network, also via Wi-Fi, with any personal or private device, must be in compliance with the IIT procedures and policies, guaranteeing application of the security measures provided for by the information security policy and related annexes. The same applies in the case of external personnel who provide services to IIT: in this case the authorisation to use the R.I. by third parties must be requested from the ICT Management by the internal contact person who is responsible for the external User, who must comply with the rules established by this procedure.

The installation and use of equipment with network connectivity, such as (but not limited to) hubs, switches, routers and access points, are prohibited unless they have been previously approved by the ICT Management: such unapproved equipment connected to the company network can be removed by the designated personnel awaiting termination of the assessment, in compliance with the admissible controls described above.

On the IIT network, Users are not permitted to carry out any scanning, interception or analysis of data traffic, nor ethical hacking activities.

5.1.4. Remote accesses

Remote access, i.e. connection to the IIT network coming from outside the IIT structures, is permitted to all Users through the Virtual Private Network (VPN) service, which provides a secure access channel to the IIT R.I. through the public network (Internet) and allows access to these R.I. remotely as if users were on the IIT premises.

The remote access service requires specific software that is pre-configured by the ICT Service Desk on assigned devices. For specific requirements approved by the ICT Management and by the Manager of an external User, the VPN service can be configured on external personal devices that will be suitably limited to the specific purpose through a nominative account and exclusively for the validity period of the requested requirement. In these cases, the external User MUST:

> [R5] ensure that the VPN software installed on their device is updated or must report its impossibility to the IIT ICT Service Desk and stop using it, while waiting for its configuration to be restored, in compliance with the measures provided for in the information security policy.

5.2. End-point

In accordance with the ICT policy (quoted, prf. 3.2), IIT allows the moderate and reasonable private use of assigned R.I.. Such use must be limited and based on common sense criteria and must not in any way compromise or hinder professional use.

IIT may, for justified reasons, decide to withdraw, reassign, replace and modify the R.I. provided to the User at any time. In such cases, the information contained in the afore-mentioned devices will be securely deleted and any software licences used will be recovered for reuse and reassignment. For no reason can a device assigned to a User be reassigned independently to another User.

Upon termination of the employment relationship, the R.I. assigned to the User will be returned to the respective ICT Contacts, who will proceed to delete the data contained on the devices through an appropriate secure deletion process within 30 days of their return. IIT may in any case retain data deemed relevant for business purposes (with the exception of personal data) in compliance with the applicable legislation and within the retention periods provided for by it.

5.2.1. Workstations

Workstation refers to the unitary complex of personal computers, accessories, peripherals and any other device provided by IIT (or authorised by the same) to the User, including any company smartphone assigned according to the "ICT procedure for assigning equipment of mobile telephony", and including the software granted for use by the User exclusively in the interest of IIT and for the performance of own duties.

The workstations must be appropriately configured according to Italian Legislative Decree 81/2008 and to the types of data that will be processed, in compliance with the "Information security policy", where possible through the use of software agents, made available centrally by the ICT Management together with the minimum configuration parameters to be respected, in relation to security configurations (antivirus/antimalware, personal firewall, device encryption, backup), with verification over time of their compliance with the configurations thus set and with management of the life cycle of the devices and applications installed.

With reference to the assigned workstation, each User therefore MUST:

[R6] immediately notify the designated structures in the event of theft or loss of the assigned devices, in accordance with the "Procedure for the Management of ICT and Log Security Incidents" and reporting the incident to the Public Security Authority. If the technology allows it, IIT can remotely deactivate the device or remove the authorisation to access the company network;

[R7] follow all the instructions given by the AdS regarding updates and critical patches for the operating system or application software, without attempting to interrupt the execution of updates or patches in the event of automatic push of the same on the devices;

[R8] always block the assigned PC with a password-protected screensaver or by logging out of the session when leaving a workstation;

[R9] set a PIN code (or equivalent, such as Face ID, fingerprint) to unlock any company smartphone supplied in order to have encryption activated when not in use;

[R10] upload any "private" files within the assigned devices, being sure to archive said files within a clearly recognisable folder (for example, calling it "*private_first-name_surname*" where possible), as defined by the "Access to data in case of sudden or extended absence". It is always the User's responsibility to ensure, where they deem appropriate, that such data is synchronised or not with the backup technologies provided by IIT, and to be aware that such files are not exempt from security controls (such as, but not limited to, antivirus scans). It is also specified that IIT cannot be held responsible in any way for the loss or dissemination of such "private" data and that in the event of termination of the employment relationship, for whatever reason this happens, such "private" data will be securely and irreversibly deleted, as it is no longer possible for the User or their successors to recover it;

[R11] protect their laptop and any other portable device against accidental damage and theft, by carrying them with them in a dedicated bag, and keeping them under lock and key or use other physical protection systems (where applicable) if they need to be left unattended for a prolonged period of time.

Similarly, the User MUST NOT:

[R12] copy, communicate or disclose IIT files or data contained on assigned devices, except in IIT's interest;

[R13] remove, copy, transfer or modify the software on their own initiative, as the software installed on the devices is subject to regular licence in accordance with the applicable laws. If this is necessary, the User must contact the ICT Service Desk to request assistance;

[R14] modify, disable, alter or circumvent software configurations and security controls installed on assigned devices, such as the configuration of anti-virus and anti-malware agents;

[R15] install programs other than those officially installed, even if they are freeware or shareware versions. Any exceptions must be requested from the ICT Service Desk so that such cases can be correctly assessed together with the ICT Management or with the relevant

Manager, for the technical requirements and compliance with internal policies and the role covered by the User within IIT. Otherwise, IIT reserves the right to uninstall the software remotely. Installing software without a regular licence is not permitted under any circumstances: IIT will not tolerate illegal use of the software;

[R16] install or otherwise use external devices on the assigned computer (such as modems, burners, MP3 players, USB sticks, Wi-Fi routers/keys, telephone hotspots, etc.) without the explicit authorisation of the ICT Service Desk. Any use, for exclusively professional reasons, of memory and/or storage media and USB sticks and other types of hardware owned by the User must be previously authorised and verified for compliance with the security measures by the ICT Management before being connected by the User themselves to the assigned computer;

[R17] transfer in use, even temporarily, the assigned or personal tools (if they also contain company information) to third parties, including other Users, nor communicate or otherwise allow third parties to learn of their access credentials or unlock codes. In general, only the personnel of the ICT Service Desk are authorised to access the devices with the prior consent of the User;

[R18] independently carry out maintenance or repairs on assigned devices or ask unauthorised personnel to perform them on their behalf. Should any repairs be necessary, it will be the User's responsibility to promptly notify the ICT Management of this;

[R19] access networks, whether wired or wireless, other than IIT networks (except in the case governed by teleworking agreements), unless this is explicitly authorised by the hotspot owner or by the network owner or provider. This restriction is aimed at avoiding potential liability or other problems due to unauthorised and therefore illegal access to a network. In particular, it should be remembered that Wi-Fi networks, both private and public, could be specially configured in order to intercept information or compromise the devices connected to them, and that due attention must therefore be paid for any access to these types of networks.

5.2.2. Bring Your Own Device (BYOD)

"Bring Your Own Device" (BYOD) describes a voluntary principle according to which it is possible to integrate private mobile devices, such as notebooks, tablets and smartphones, for access to corporate R.I. - whether they are equipped with corporate SIMs or data connectivity owned by the User. IIT allows its Users to use their devices as part of the activities carried out on behalf of IIT: for this purpose, each User must ensure compliance with the security measures provided for by the Foundation's information security policy.

The ICT Management provides support for the correct initial configuration of the personal device and is required to check its compliance, for example by installing a software agent, in compliance with the protection of the P.D. present on the device and excluding any remote control on the activity of the User. In the absence of compliance with the security requirements, it is in any case the right of IIT to block the connections of the personal device to the corporate R.I..

If the authorisation to use personal tools is revoked, for example if the professional relationship with IIT ceases, the IIT company data present on the User's device must be deleted by the User themselves with the support of the ICT Management, or securely remotely using the software agent, if previously installed.

The requirements [R6], [R7], [R8], [R9], [R11], [R12] and [R13] formulated in section 5.2.1 also apply to devices in BYOD mode and the Users must therefore observe such prescriptions, wherever they are. In addition, considering the specific risks that BYOD can create, further rules for its correct use are outlined below. In particular, the User MUST:

> [R20] only install and use company software on personal devices if permitted by the End-User License Agreement (EULA) or if authorised by the ICT Management;
>
> [R21] keep private information completely separate from that relating to work, by configuring appropriate dedicated workspaces.

Similarly, the User MUST NOT:

> [R22] modify or circumvent the security configurations regarding device encryption and virus protection, nor disable the presence of the unlock code;
>
> [R23] introduce private information present on personal devices into IIT servers in order to avoid creating breaches of the User's confidentiality and to avoid risks and responsibilities, even if only potential ones, on the security of the IIT infrastructure.

5.2.3. Removable devices and media

The use of external devices, whether connected to the network or not, such as printers, copiers and faxes, must always be used for business purposes. In particular, the User MUST:

> [R24] collect copies immediately as soon as they come out of the printer, paying particular attention when sending documents relating to P.D. or to confidential information to a shared printer; where available, the use of multifunction printers with access protected by the use of a badge is required.

Similarly, the User MUST NOT:

> [R25] use fax machines to send documents that are confidential in nature. In cases where this is strictly necessary, the User must first notify the recipient and ask them for confirmation of receipt and must also await the receipt of sending issued by the fax itself.

With regard to the storage media entrusted to Users for business reasons, such as USB sticks, CDs, DVDs, removable hard disks, they are tools owned by IIT and must only and exclusively be used in the interest of IIT and for the performance of the tasks assigned to each User. Where applicable, these media are suitably pre-configured (for example by encrypting the medium itself) to ensure a level of security appropriate to the possible type of data processed, in particular with regard to P.D. or high-risk data, also qualified by the information security policy.

The requirements [R6], [R11], [R12], [R13], [R14], [R17] and [R18] formulated in section 5.2.1 also apply to removable media and therefore the Users must comply with these requirements, wherever they are and where appropriate. In addition, the User MUST:

[R26] only upload company data and files to removable media if they are relevant to their role and in response to an explicit need, and only if such storage has been authorised;

[R27] ensure the availability of a second copy of the data loaded on the removable media before their elimination or destruction or in any case for reasons of business continuity, to prevent their unavailability in the event of loss or failure of the media;

[R28] scan removable media every time they are used, where not automatically provided, in order to scan for viruses and other malware. This search must be performed before accessing, uploading or downloading data or files to or from the removable media;

[R29] ensure that sharing of files and data through the removable media is only performed with persons authorised to access the data being shared.

Similarly, the User MUST NOT:

[R30] allow third parties to use the removable media supplied to them without the User's supervision, as even deleted files and data can potentially be restored or read through the use of specialised software;

[R31] use removable media of whose origin they are unsure, as they could be infected with malware and constitute a "trap" for an attacker to infect the target PC and obtain undue access to its content and to the networks to which it is connected.

5.3. Network tools

This chapter governs the methods of use and access to the IIT network and the services that, through the network, can be received and offered inside and outside the network itself. The IIT electronic network is part of the national electronic network infrastructure called "GARR Network - The Italian Network of University and Scientific Research", in relation to which it uses the connection and interoperability services that allow access to the Internet. Use of the IIT network is therefore subject to compliance by all Users not only with this Procedure but also with the rules dictated by the "Acceptable Use Policy" of the GARR network.

5.3.1. Internet

Users are normally permitted to access the Internet through the assigned R.I. only and exclusively in the interest of IIT and for the performance of the related duties or professional collaboration activities being exercised. IIT, until further and different communications, allows personal use of the Internet provided that such use is moderate and based on common sense criteria, and that it takes place in such a way as not to compromise or damage the work performance and functionality of the R.I. from which access takes place, or the company network itself and the data contained therein. IIT reserves the right to make any assessment regarding the tolerability threshold of the overall use of the network.
In order to prevent the risk of improper use of Internet browsing, consisting of activities not related to work performance, IIT uses a system of filters (even at the individual device level) that prevent certain operations such as the viewing of illegal websites, the uploading or downloading of files with particular characteristics (size or type of data downloaded) and the use of network services for recreational purposes or for purposes unrelated to work. For these reasons, any direct access to the Internet (through the use of external or internal modems or other devices) made by bypassing the security systems adopted by IIT is not authorised.
Furthermore, for operational, legal and security reasons, and in compliance with the current legislation and regulations regarding the protection of P.D., IIT can monitor Internet traffic, automatically analysing it to block viruses and other harmful content and keeping logs thereof in compliance with the provisions of paragraph 4.2 "Permitted controls".

During the use of Internet services, the following behavioural rules must therefore be observed, and in particular the User MUST:

> [R32] comply with copyright laws and have in advance the necessary user licences applicable to software or other material personally downloaded or copied.

Similarly, the User MUST NOT:

> [R33] make illegal use of the Internet, or even exercise improper use that could be a source of damage for IIT or that could damage its interests or reputation or that could be a source of responsibility of IIT and/or of the User, in particular in terms of secrecy and confidentiality of company data or breaching of the principles of employee loyalty, or compromising the security of the company network;
>
> [R34] carry out activities that could harm or breach the confidentiality or privacy of other Users, for example by making unauthorised scans or searching for or disseminating statements or illustrations that are offensive, defamatory, unconstitutional, racist, sexist, that incite violence or that are pornographic;
>
> [R35] access or provide contact details to websites whose contents are not related to professional activities using credentials used in the workplace, nor use or reuse personal credentials (ID and password) for registration on websites, apps or work services, nor in general assume a false identity on the web;

[R36] change the security settings of applications used for Internet access or applications that control Internet access (for example, antivirus).

5.3.2. E-mail

E-mail is an essential service for IIT Users and therefore each User is assigned a nominative and personal mailbox. However, use of the e-mail box provided is exclusively professional and is not for private use as it is part of a company-owned tool and functional exclusively to business needs. E-mail messages, their identification data, contents and attachments therefore constitute, also in the context of the above, expression and manifestation of the work activity and are to be considered to all intents and purposes company documents and as such are the exclusive property of the company. It is therefore not permitted to use the e-mail box, even if outside working hours, for private purposes, or in any case for purposes not related to the performance of the assigned tasks. Prohibition of the use of e-mails for private purposes also entails, in order to avoid receiving messages not relating to work activity, the prohibition of disclosing, disseminating and/or communicating one's own corporate email address to subjects who are not involved in relations relating to the work activity.

In case of prolonged absence, each User must adopt adequate measures to ensure correct management of the messages required for the continuation of the normal work flow, in accordance with the rules of this procedure. In particular, each User can identify a delegate to access for such cases, without prejudice to IIT's right to access the User's mailbox if this is deemed necessary for extremely important business requirements and where the preferential alternatives provided for in the "Access to data in case of sudden or extended absence" are not practicable, in compliance with what is described in paragraph 4.2.1.

In the event of termination of the employment relationship, the User's mailbox will be immediately deactivated, and an automatic reply message will be prepared informing the sender of the termination of IIT's relationship with the User. At the request of the User and subsequent evaluation by the HCO and ICT Departments, the automatic message may contain a reference to a private e-mail address of the User. In any case, after six months of deactivation, IIT will order final and total deletion of the mailbox.

To ensure the security of information passing through IIT, the latter uses an anti-spam filter capable of blocking incoming or outgoing e-mail messages deemed undesirable/unreliable, or those with attachments larger than those technically permitted by the service (according to the provisions of the service sheet, available on the Intranet page https://intranet.iit.it/offices/information-and-communication-technology/e-mail-calendars/e-mail-service). Each User must therefore be aware that some information relating to the use of the e-mail service, such as sender, recipient and subject, may be present in the tracking logs. It is therefore advisable to avoid entering personal information in the e-mail subject.

Similarly, and although IIT makes every reasonable effort to protect the mail system in its entirety, e-mail messages to addresses external to IIT can travel in cleartext for reasons inherent in the very protocols for transferring messages via the Internet. The message sent must therefore be considered as open mail, so the confidentiality of its content is not guaranteed, nor of the identification data of the sender or recipient.

The safe behaviour adopted by each individual User is therefore essential to guarantee an acceptable level of security for the e-mail platform as well as for individual communications.

In particular, the User MUST:

[R37] guarantee the confidentiality of communications to external addresses when the sending includes P.D. or high-risk data (according to the Information Security Policy) by encrypting the message or protecting it on files with restricted access;

[R38] always check that they have entered the correct e-mail address of each recipient before clicking 'Send', being very careful when using group e-mail or the 'Reply to all' or 'Forward' function, limiting the text of the e-mails to the subject that has been identified and avoiding giving information that is extraneous to it or that the recipients of the forwarded e-mails may not be authorised to see;

[R39] be careful when opening attachments or clicking on links contained in an e-mail, especially if received from unknown senders, as they may contain malicious code or code that deceives into revealing passwords and personal information;

[R40] be wary of unsolicited e-mails requesting personal or financial information as they may be phishing attempts, as well as e-mails sent by seemingly authentic senders but containing an unusual message body, such as requests for money or unusual internal transactions, as this could be scam;

[R41] always contact the ICT Service Desk if in doubt, without replying to suspicious emails.

Similarly, the User MUST NOT:

[R42] use the electronic mail tool in an improper or illegal manner that could be a source of liability, for example, in terms of secrecy and confidentiality of company data or breaching of the principles of loyalty typical of employment relationships (from the perspective of unfair competition, unauthorised work, etc.);

[R43] perform e-mail forwarding and/or automatic redirections to private accounts;

[R44] attach potentially non-secure material (e.g., executable programs, scripts, macros) as well as oversized files, which could be classified as unwanted (spam), to e-mail text;

[R45] use, regardless of whether for receiving or sending, private mail accounts for business purposes;

[R46] use corporate e-mail addresses to participate in on-line debates, forums, mailing lists, etc. that are not part of the work activity or for the propagation of message chains (even if for charitable purposes), unless expressly authorised by IIT;

[R47] use images or language that could be considered obscene, deceptive, defamatory, racist or that could be used to determine P.D. or sensitive data of third parties;

[R48] use mail folders saved locally on the PC (such as *.pst* files in MS Outlook) as the primary repository of the mailbox in use, whenever this is technically possible.

5.3.3. Collaboration tools

IIT manages a set of network services, both on-premise (shared access network folders) and in the cloud, to facilitate collaboration and information sharing among its Users, such as videoconferencing services (for example, Microsoft Teams) and storage services (for example, Microsoft Sharepoint and Microsoft OneDrive).

These tools are dedicated to the processing only of data and information owned by IIT, are for strictly professional use and cannot in any way be used for different purposes, and in any case always in compliance with the limits permitted by this Procedure and by the other IIT policies in force, with particular regard to the Information Security Policy and to the protection measures for classified data.

Access to these tools takes place through the company credentials referred to in paragraph 5.1.1, and through the R.I. assigned to the User referred to in paragraphs 5.2.1 and 5.2.2. All related provisions and rules of correct use defined in these paragraphs are therefore also applied in this area and form an integral part thereof. In addition to this, the User MUST:

[R49] obtain consent prior from interested parties to the recording of meetings and events, wherever they wish to activate this service (not active by default);

[R50] limit access to IIT information only to subjects who are entitled to it on the basis of the "need-to-know" principle, in particular avoiding any form of sharing "with everyone" of IIT information not intended for publication or dissemination - for example, it is possible to allow access levels to individual files or to individual third-party Users even in "read-only" mode.

Similarly, the User MUST NOT:

[R51] use collaboration services that have not been provided or otherwise previously approved by the ICT Management;

[R52] place files of any kind on the collaboration services that are not directly related to own duties and that are not necessary or functional to their execution.

The User must also be aware that the information saved on these tools will be precluded from their access upon termination of the collaboration relationship with IIT and that in any case the information on workspaces to which they have exclusive access may be permanently removed from the afore-mentioned services (on-premise or even in the cloud) within 60 days from the deactivation of the account authorised to access it. If it is necessary for operational continuity of access to company data, the procedure "Access to data in case of sudden or extended absence" will be applied.

5.4. Handling exceptions

The ICT Management may only evaluate and grant exceptions to the rules in this procedure if they refer to needs and requirements dictated by particular working conditions, evaluating them on a case-by-case basis with the contact persons of the applicant. Under no circumstances can exceptions be granted in relation to compliance with the applicable laws or regulations. All exceptions granted by the ICT Management are formally authorised in writing and are tracked by the ICT Management itself.

5.5. Final provisions

Verification of compliance with the rules established in this procedure regarding the correct use of R.I. and the periodic assessment of controls and their effectiveness, in order to facilitate the identification of risks and the definition of appropriate mitigation actions, is the responsibility of the ICT Management.

This procedure comes into effect from the date of publication.