ISTITUTO
ITALIANO DI
TECNOLOGIA

Logical Accesses Procedure

Revision	Description of Modification	Author	Approval	Date
01	First issue	ICTD	SD DG	13/05/2019

SUMMARY

1. Objectives and purposes 3
2. Introduction and definitions 3
2.1 Introduction 3
2.2 Definitions 4
3. Main actors and responsibilities 4
4. Documents and tools 5
5. Actuation 6
5.1 Principles 6
5.2 Authorisation Profiles and Personal User Accounts 6
5.3 Management of Authorisation Profiles 7
5.4 Management of Personal User Accounts 8
5.5 Management of Administrative User Accounts 10
5.6 Management of Technical User Accounts 10
5.7 List and Revision of all User Accounts 12
5.8 Security Measures for Logical Accesses 12
5.9 Control activities 13
5.10 Responsibility 13

1. Objectives and purposes

- The object of this Procedure is the management of the user accounts that allow access, use and management of all the IT and telecommunication systems and equipment (hereinafter also "Information Systems") owned by or available to the IIT Foundation (below, also "Foundation" or "IIT").
- The recipients of this Procedure are any persons who have an employment or collaborative relationship and external personnel affiliated to the IIT Foundation who carry out scientific, professional or study research within the IIT facilities. The afore-mentioned categories of subjects will also be referred to as "Users" below.
- The recipients of this Procedure are also all third parties, such as suppliers and research organisations, which manage information from the IIT Foundation through IT and telecommunications systems and equipment. The afore-mentioned categories of subjects will also be referred to below as "Third Parties".
- The purpose of this Procedure is to establish rules for the creation, management, assignment and removal of privileges and user accounts in the IT systems of the Foundation, in order to ensure that security measures are satisfied that mitigate possible risks related to the Confidentiality, Integrity and Availability of information and of IT systems.

In the following provisions, reference will also be made to the applicable legislation in force regarding the protection of personal data.

2. Introduction and definitions

2.1 Introduction

The Foundation adopts tools, processes and procedures useful in order to guarantee the security of information and to encourage the taking of responsibility by individual users.

The Information Systems made available to Users by the Foundation constitute one of the strengths of the latter but at the same time they can be a source of risk for the security of the information processed and for the image of the Foundation. For this reason, the management of the user accounts that allow access to the IT systems of the Foundation must follow procedures that mitigate the risks related to the Confidentiality, Integrity or Availability of information and IT systems owned by or available to the Foundation .

2.2 Definitions

Name	Abbreviation	Description
Information and Communication Technologies	ICT	Information and Communications Technology", ICT, are the set of methods and techniques used in the transmission, receipt and processing of data and information usually through digital techniques and tools.
IT systems	C.S.	The IT and telecommunications systems and equipment owned by or available to the IIT Foundation.
Telecommunication Network	T.N.	The set of devices and their connections (physical or logical) that allow the transmission and receipt of information of any type between two or more user accounts located in geographically distinct positions, transferring them via cables, radio systems or by other electromagnetic or optical systems.
Personal Data	P.D.	Any information relating to an individual, identified or identifiable, even indirectly, by reference to any other information, including a personal identification number.
User	US	A user is a natural person who interacts with a C.S., accessing it via a user account.
User account	Us.a	A user account is an IT mechanism through which a C.S. provides a user account, identified by a user name, with a processing environment possibly with customisable contents and functions and with appropriate isolation from other user accounts.
Technical User Account	Te.U	A technical user is a user that is not associated with a natural person and is typically used to manage a C.S.
Personal User Account	Pe.U	A personal user account is a user account that is uniquely assigned and used by one physical person only.
Administrative User Account	Ad.U	An administrative user account is a user account that allows the administration and management, such as installation and updating, of a C.S. and of its components.
Authorisation Profile	A.P.	An authorisation profile is a set of privileges that allow assigned user accounts to perform a coherent set of activities on a C.S.
Active Directory	AD	Active Directory is a set of network services present in Microsoft systems that centrally manage the user accounts and resources of the C.S. through Group Policies.
AD domain	AD.D.	An AD domain is a logical group of Microsoft C.S. that share a centralised AD database directory.
Remote Access	RA	Access to a system, service or application present or supplied by a device other than the one physically used by the user account or directly connected to it.
Strong Authentication	SA	An authentication method that uses methods that are safer than simply checking the password, typically using at least two checks: a thing that is known (such as a password), something owned (such as a physical device, key, etc.), a physical attribute (such as a biometric feature of the user).

3. Main actors and responsibilities

Actor	Abbreviation	Main responsibilities
ICT Directorate	ICTD	The development and management of the internal network is entrusted to the ICT Directorate which operates in accordance with the resolutions of the institutional bodies of the Foundation and in close collaboration with GARR. The ICT Directorate centrally manages the privileges and/or user accounts of the C.S. in AD. domain.
User	US	Anyone who has an employee or collaborative relationship and external staff affiliated to the IIT Foundation that carries out scientific, professional or study research within the IIT structures. Users of the Foundation's network are in particular persons that belong to all the research and service structures directly connected to the internal network of the Foundation. All users who use the Foundation's network for any reason accept this Procedure without reservation.
Director	DIR	Each Director/Department Manager validates and authorises the creation, modification, closure and removal of user accounts and privileges on the systems for which they are responsible.
Principal Investigator/ Facility coordinator	P.I.	Each P.I. validates and authorises the creation, modification, closure and removal of user accounts and privileges on the systems for which they are responsible.
System Administrator	S.A.	Particular users of the C.S. with responsibility for the management and administration of the same, as also defined by the General Provision of the Privacy Guarantor of 27 November 2008
Human Resources and Organisation Department	H.R.O.D.	The Human Resources and Organisation Department informs the ICT Directorate of the requirement to create a new user account, to change a user account (for example to change the job), and to close a user account due to termination of the employment relationship for the systems managed by the ICT Directorate.
ICT Referent	R.ICT	A technical figure assigned to the management of C.S., not managed directly by the ICT Directorate.

4. Documents and tools

Type	Name	Use
Policy	ICT Policy	To establish the correct use of IT systems in the IIT Foundation (hereinafter, also "Foundation" or "IIT") protecting IIT and Users from the risk of compromising IT Systems, from undue disclosure of personal and confidential data and from the related legal consequences.
Procedure	Access to data in case of emergency or prolonged absence	Defining and regulating, in accordance with the Foundation's ICT Policy, the methods of accessing company data, managed by Users, located within the Foundation's IT systems, in the event of the sudden or prolonged absence of the User during which there may be unavoidable needs linked to the work activity or from which, in any case, harmful consequences for the Foundation may arise.

5. Actuation

5.1 Principles

The management of personal user accounts and access rights to the Foundation's systems and applications is based on the following principles of security and good governance of the systems:

1. "Need to know" principle:

   The right of access to a system or application is granted only to those who need it to manage the system itself or to manage the business processes and the information present therein;

2. Principle of minimum privilege:

   The privileges granted for access to a system or application must be limited only to those essential and necessary to perform the activities assigned to the User;

3. Principle of separation of duties:

   Personal user accounts can be assigned privileges related to only one of the following three functions: operational, authorisation, control.

The three principles must be applied based on the actual needs of the Foundation, for example it may be the case that principles 2 and 3 do not apply to certain System Administrators, and that principle 3 does not apply to certain Directors or P.I.

5.2 Authorisation Profiles and Personal User Accounts

In each system and application, Authorisation Profiles must be defined, that is, sets of privileges that permit a personal user account to whom a coherent set of activities have been assigned to perform.

The main privileges allow the creation, modification, reading, cancellation or execution of a set of resources. An Authorisation Profile indicates, for each set of system resources or application, which privileges are granted. By default, no profile is granted any privileges to all the system or application resources (in accordance with the principle of minimum privilege). The configuration of a profile consists of the assignment of only those privileges necessary for management of the resources useful for executing a coherent set of activities.

One or more profiles are associated with each personal user account.

For the management of Authorisation Profiles and of user accounts it is necessary to specify the relationship between the C.S. and the corporate AD domain; three cases are possible:

1. C.S. integrated in the corporate AD domain both for authorisation user accounts and for profiles: authorisation user accounts and profiles are created in the AD domain and shared by it with the C.S.;
2. C.S. integrated in the corporate AD domain only for user accounts: user accounts are created in the AD domain and shared by it with the C.S. while the authorisation profiles are created and managed directly in the C.S.;
3. C.S. not integrated in the corporate AD domain: both the authorisation user accounts and profiles are created and managed directly in the C.S.

Where technically possible, both authorisation user accounts and profiles must be integrated within the corporate AD domain.

5 types of personal user accounts are possible:

1. Central administrative user accounts: user accounts employed by the S.A. to manage systems and applications associated with the corporate AD domain;
2. Local administrative user accounts: user accounts used by the S.A. to manage systems and applications local to the system or application;
3. Personal user accounts in the AD domain with central profiling: user accounts and profiles managed through the corporate AD domain;
4. Personal user accounts in AD domain with local profiling: user accounts managed through the corporate AD domain with profiles managed locally on the system or application;
5. Local personal user accounts with local profiling: user accounts and profiles managed locally on the system or application.

Where technically possible, central user accounts and profiles in AD domain must be used.

5.3 Management of Authorisation Profiles

For each C.S., the management of authorisation profiles, both local and through the corporate AD domain if integrated, consists of the following operational steps.

Creation, modification or removal of an authorisation profile

- The request to create, modify or remove an authorisation profile is formulated by the manager of the C.S. as a party charged with evaluating the opportunity and need for a new profile or the need to make changes to an existing profile, so that the profile constitutes a set of privileges and resources useful for executing a coherent set of activities;
- The manager of the C.S. coordinates with the development group for the implementation of the new profile or, where not necessary, with the S.A. for the direct implementation of the profile on the C.S.;
- The development group, or the S.A., creates, modifies or removes the authorisation profile on the C.S.

List of authorisation profiles

The manager of a C.S. must be able to provide the list of existing authorisation profiles on the C.S., associating with each profile the description of the purpose and the privileges granted, also through extraction from the C.S. carried out by the S.A. or by another reference technician.

Review of authorisation profiles

- For each C.S. at least once a year the list of authorisation profiles is produced and a review of all existing authorisation profiles is carried out;
- The manager of a C.S. evaluates if there are authorisation profiles to be modified in which case it is necessary to proceed according to what was previously described in this section;
- The manager of a C.S. evaluates if there are authorisation profiles to be removed, for example if an authorisation profile is no longer assigned to any user account and it is not expected that new user accounts will be created to use them; to remove the authorisation profile proceed as described above in this section.

Some systems, such as SAP and related analysis and reporting systems, require the management of specific authorisation profiles, the details of which are presented in a dedicated procedure that replaces this section.

5.4 Management of Personal User Accounts

Each personal user account on the C.S. is individual and shared accounts are not permitted. Each personal account must be documented in a work or supply contract.

A personal account cannot exceed the expiry of the contract with the Foundation of the user to whom it is assigned.

When creating a new personal user account, the S.A. creates a new, complex[1] and unique password for the account that it communicates to the User. Upon initial connection the user must change the password.

Where technically possible, systems and applications should prompt users for authentication after a predefined period of inactivity, typically set at 15 minutes [2].

If users are assigned profiles that allow access to personal data [3], before enabling user access to the C.S. it must be verified that the user has been appointed and has accepted the appointment as a person responsible for the processing of personal data.

The management of personal user accounts includes the following activities.

Creation or modification of a personal user account on C.S. integrated in AD domain (preferential system)

- For the C.S. integrated in the AD domain of the Foundation the creation or modification of a user account is carried out in AD; the Human Resources and Organisation Department updates and verifies the shared registry of the users of the Foundation, specifying the contractual deadline;
- The manager of the C.S., or the person responsible for the user requesting creation of the user account, indicates the authorisation profiles to be assigned to the account;

[1] See section 5.8 "Security Measures for Logical Access".
[2] See NIST 800-53 (Rev. 4) AC-11 "Session Lock", and Australian Government Information Security Manual Control 0428 "Session and screen locking"
[3] See the applicable legislation in force regarding the protection of personal data.

- The S.A. creates the user account in AD with the profiles indicated and, if requested, assigns to the user additional local profiles on the individual systems;

Creation or modification of a personal user account on C.S. not integrated within the AD domain

- For systems and applications that are not integrated within the corporate AD domain, the C.S. manager, asked by the Human Resources and Organisation Department for an opinion, collects the user's personal data, expiry, qualification and duties and indicates to the S.A., authorising it the authorisation profiles to be assigned or modified in relation to the user account;
- The S.A. of the C.S. creates or modifies user accounts with the profiles indicated.

Closure of a personal user account

Upon expiry of the validity of the contract, the user accounts are automatically closed by the C.S. integrated within the corporate AD domain. For C.S. not integrated within the corporate AD domain, the manager of the C.S. instructs the S.A. to close the user account upon the expiry date of the same.

Temporary block of a user account

The manager of the C.S. can ask the S.A. to temporarily block a user account in the event of incidents, suspicious activity, for security or urgency reasons, notifying the interested party and the Human Resources and Organisation Department thereof.

At the end of the temporary block of the user account this can be closed or reactivated in which case it must be evaluated if it is necessary to reset the password.

Password reset of a user account

Where present, a user can use the autonomous password reset service provided via a dedicated portal, or they can request the reset of their user password from the ICT Directorate, or directly from the C.S. S.A..

For security reasons, the ICT Directorate may impose a password reset on some or all user accounts.

In the event of a non-autonomous reset of the password, a user requests a reset for their own user account from the ICT Directorate via ticket or directly from the S.A.. The S.A. creates a new password that is complex[4], unique for that user and which communicates to the user; upon first access that they must change the password.

[4] See section 5.8 "Security Measures for Logical Access".

5.5 Management of Administrative User Accounts

Administrative user accounts for all the Foundation's systems and services are nominal and individual; shared administrative user accounts are not permitted.

Administrative user accounts are distinct from personal user accounts and must be used only for the administration and management activities of C.S.

Administrative user accounts can only be assigned to personnel who have been appointed as S.A..

Where technically possible, access to administrative accounts must be made with Strong Authentication (see section 5.8).

Access and administrative tasks must be tracked. Activity tracking must comply with current legislation.

The process of emergency access to systems and applications is described in the appropriate procedure.

Although not specified in this section, the management of administrative user accounts follows the process described in section 5.4.

5.6 Management of Technical User Accounts

Technical user accounts are service accounts created on the C.S. typically to carry out administration, management and interfacing activities to allow the execution of specific applications or to permit the execution of technical activities within the C.S. themselves.

Technical user accounts can be assigned administrative privileges.

The manager of the C.S. is also responsible for any technical user account present in the C.S., their management as described here and the adoption of the security measures described in section §5.8.

Technical user accounts must not be used by users for normal activities on IT systems or for activities not included in the scope predefined for each of them.

It is envisaged that the System Administrators access the C.S. locally. (e.g. through a system console), using technical user accounts, in the following exceptional cases:

- when network connectivity is not available for remote access to the C.S. by the System Administrators through their nominal utilities;
- for needs related to ordinary or extraordinary maintenance of the C.S. by System Administrators, where it is not possible to carry out these activities remotely, using their nominal user accounts.

Local access (from the console) to the C.S. by the System Administrators through technical user accounts, in the exceptional cases previously indicated, is subject to the adoption of suitable procedures to ensure:

- the certain identification, also physical, of the System Administrator who will be using the technical user account;
- the justification and the purpose of the activities that require the use of impersonal user accounts;
- the recording of the date and time of access and the unambiguous identification of the system(s) concerned;

- recording of the time interval (login-logout) during which the Administrator used the impersonal user account;
- adequate keeping of the passwords associated with impersonal user accounts, aimed at guaranteeing their confidentiality and, at the same time, their availability when there is a requirement to use them;
- temporary validity of the password used for access, limited to a single intervention session.

Technical user accounts can be:

1. Technical user accounts in the AD domain: user accounts managed through the corporate AD domain;
2. Local technical user accounts: user accounts managed locally on the C.S.

Where technically possible, technical user accounts must be used in the corporate AD domain.

Creation of a technical user account on C.S. integrated within the AD domain

The creation of a technical user account in the corporate AD domain is authorised by the ICT Directorate and is carried out by an S.A. with the assignment of the profiles and privileges necessary both in the corporate AD domain and possibly in individual systems.

Creation of a technical user account on C.S. not integrated within the AD domain

The creation of a technical user account on systems not integrated in the corporate AD domain is authorised by the manager of the C.S. and is carried out by an S.A. with the allocation of profiles and necessary privileges.

Credential management for technical user accounts

Credential management for technical user accounts can be of the following types:

- Login blocked, access to the user account is only permitted to the S.A.;
- Login permitted by password, the password can be without expiry but should not be normally employed by users to access the user account. Access to the user account is only permitted to the S.A.; the password must be saved securely, for example in a sealed envelope in a locked cabinet.

Where present, passwords must meet the minimum security features described in section §5.8, with the exception of periodic modification requirements.

Closing and removal of a technical user account

Technical user accounts do not typically have a predefined validity. At the end of their usefulness, technical user accounts must be removed automatically with the removal of the service, or manually by the S.A. at the time of removal of the IT service to which they are assigned.

5.7 List and Revision of all User Accounts

List of all user accounts

The manager of a C.S. must be able to provide the list of all user accounts (personal, administrative and technical) that exist on the C.S., with the list of assigned profiles associated with each of them.

Revision of user accounts

- For each C.S. at least once a year the list of all existing user accounts is produced and reviewed;
- The manager of a C.S. evaluates if there are user accounts that need to be modified, for example by changing the assigned authorisation profiles, in which case the relevant process is described in the previous sections of this document;
- The manager of a C.S. evaluates, for personal and administrative user accounts with the support of the Human Resources and Organisation Department, if there are any unused user accounts that must be closed, in which case the relevant process is described in the previous sections of this document.

5.8 Security Measures for Logical Accesses

In the dialogue via network between 2 distinct systems, the access credentials must never be transferred unsecured but through encrypted channels. Accesses to remote C.S. must be performed via encrypted connections. The encryption of credentials and communications must adopt protocols and cryptographic algorithms considered safe for the current state-of-the-art.

The basic method for identifying, authenticating and authorising a user account on a C.S. is the use as a credential of a username and a password, where the password is known only to the user.

Access, especially if from the Internet, to C.S. that manage personal, confidential, particular data and in general with a high level of risk, must be permitted, where possible, by the Strong Authentication of user accounts. An authentication is strong if in addition to or in place of the password verification, at least one of the following is verified:

- something you have (for example a physical device, key, etc.);
    - particularly safe are the systems that produce additional passwords that can be used only once and for a limited time (Time-Based One-Time-Password)
- a physical attribute (for example, a biometric feature of the User).

Minimum password security features:

- Minimum length 8 characters;
- It must not contain the first name, surname, e-mail address or user identification code;
- It must contain characters belonging to at least three of the four categories listed below:
    - Upper-case letters (from "A" to "Z");
    - Lower-case letters (from "a" to "z");

- Numbers (0,1,2…);
- Punctuation (,;.:) or special characters (for example: _,-,!,$, #, %).

The password must be changed the first time it is used. In case of processing of personal or confidential data, the password is modified at least once every three months.

5.9 Control activities

The ICT Directorate is authorised by the Foundation to verify the adequacy of the definition of the authorisation profiles, the assignment of user accounts to the profiles and correct management of the profiles and user accounts as described in this document (see also the "ICT Policy").

5.10 Responsibility

Anyone who fails to comply with this policy may incur immediate suspension of access to IT systems by the IIT Foundation, which reserves the right to activate disciplinary procedures, subject to the relevant conditions.

Furthermore, violations of safety regulations in the management and use of IT systems and rules on the protection of personal data may result in further and autonomous civil, criminal and administrative consequences.