Automatically translated by DeepL

Information Security Regulation and Use of IT resources

Glossary

Computer incident	A computer incident is defined as a general class of unforeseen and (even accidental) hardware or software malfunctions.
Malware	Programme, document or e-mail message capable of cause damage to a computer system.
Data Breach	A breach of security leading - accidentally or unlawfully - to the destruction, loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. A breach of data personal may compromise the confidentialityintegrity or availability of personal data.
Athenaeum Domain	unique name placed after the @ symbol in email addresses that identifies the organisation managing it (e.g.: unipr.it).
Cloud computing	is an IT infrastructure model that makes available, via the Internet, a set of hardware and software resources (e.g. networks, servers, storage resources, software applications) that can be rapidly delivered as a service, enabling the user not to have to worry about, for example, how to configure and install software on their machine. The most common classes of service that characterise cloud services are IaaS, PaaS and SaaS. These services can be delivered to in different ways: public cloud, private cloud and hybrid cloud.
ICT	information and communications technology, are set of methods and techniques used in the transmission, reception and data and information processing (including digital technologies).
VPN	virtual private network, a private telecommunications network that guarantees various types of data protection, including confidentiality, integrity, authentication and protection from replay attacks (a form of cyber attack targeting computer networks for the purpose of to take possession of an authentication credential).
HTTPS/TSL/SFTP connections	protocols for secure communication over a computer network used on the Internet.
LOG	sequential and chronological recording of operations performed, whether by a user, administrator or automated, as they are carried out by the system or application.
IDS	Intrusion Detection System is a software and/or hardware device used to identify and/or prevent unauthorised access to computers or local networks.
Router	network device used as an interface between different sub-networks such as an Internet connection.
Wi-Fi	is a set of wireless local area network (WLAN) technologies based on the IEEE 802.11 standard, which enables multiple devices (e.g. personal computers, smartphones, smart TVs, etc.) to be connected to each other them via radio waves and exchange data.
NAS	network attached storage is a network-attached device whose function is to allow users to access and share a common space (a mass memory).
IP address	Internet protocol address is a number that uniquely identifies an device called a host connected to a computer network that uses

	Internet Protocol as a network protocol routing/addressing.
Gateway	is a network device that connects two computer networks of different types
Netmask	within a TCP/IP network, is a configuration parameter that defines the size (understood as an address range) of the IP subnet, or subnet, to which a host belongs.
DNS	Domain Name System is a system used to assign names to network nodes (e.g. www.unipr.it).
Mac Address	also called physical address, Ethernet address or LAN address, is a code uniquely assigned by the manufacturer to each ethernet or wireless network produced in the world.
DHCP	Dynamic Host Configuration Protocol is an application protocol that allows devices or terminals in a given local network to automatically receive, at each access request, from an IP network, the IP configuration needed to establish a connection and operate on a wider network based on Internet Protocol.
GARR Network	Italian ultra-wideband network dedicated the education community, research and culture.
Single sign on	unique authentication or unique identification is the property of an access control system that allows a user to make a unique authentication valid for several software systems or computer resources to which it is enabled.

Foreword

The University of Parma (hereinafter referred to as the University) considers the adoption of information and telematic technologies indispensable for the performance of its institutional activities and for the constant improvement of the services offered to users, and also believes that the use of the Internet is an indispensable tool to ensure the widest visibility and dissemination of information relating to its institutional activities.

The University must adopt appropriate controls to protect the confidentiality, integrity and availability of data in accordance with good practices and standards on information security, in compliance with existing regulatory obligations (copyright laws, privacy laws *D.lgs 196/2003* updated to *D.lgs 101/2018 - Personal Data Protection Code, European Regulation - EU Regulation 2016/679 of the European Parliament L. 119 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* published in the OJEU of 04 May 2016 (hereinafter GDPR), *Legislative Decree 7 March 82/2005* as amended - *Digital Administration Code*, *Circular 18 April 2017, no.2/2017*, on "Minimum ICT security measures for public administrations" *Directive of the President of the Council of Ministers 1 August 2015*).

Therefore, given that the use of IT and telematic resources must always be inspired by principles of responsibility, diligence and fairness expressed in the ***Code of Ethics*** and must be aimed exclusively at activities envisaged within the framework of institutional, administrative, teaching and research activities, the University has adopted an internal policy for the implementation and dissemination of a culture of IT security to protect the **integrity**, **availability** and **confidentiality of information**.

The University provides its users with services through various types of IT resources. These are described in the ***IT Services Catalogue***. These regulations define the conditions for accessing and using the University's IT services and resources; for the specific aspects of certain services, please refer to the relevant regulations.

1. Objectives

These regulations have the following objectives:

- **prevent**, where possible, even unconscious conduct that could threaten or compromise the security of data processing, compliance with copyright law, and/or access to University resources;
- **codifying** the rules of conduct to be followed for the correct use of tools and services in order to avoid problems, inefficiencies, additional costs and risks to the security the University's data and assets;
- **preserve** security in accessing the internal network and the Internet;
- **ensure** compliance with the laws on the use of IT resources for the processing of personal data in accordance with the GDPR, related Privacy Guarantor Measures and national sector regulations;
- clearly **inform** stakeholders about monitoring and control activities;
- **disseminate** a safety culture that contributes to achieving and maintaining the highest quality levels of services rendered.

2. Scope of application

These Rules and Regulations apply to the entire University, for all its locations and cover all human, physical and virtual resources.

This Regulation is intended for individuals and personnel involved in various ways in the activities of the University and for all those who use the University's ICT services, and defines the policies adopted to guarantee the security of information directly by the University, with which the suppliers/outsourcers of services/activities functional to the provision of ICT services must also comply.

By way of example and not limitation, parties concerned may be:

- Lecturers (Full Professors, Associate Professors, Researchers, Emeritus Professors, Honorary Professors);
- Technical Administrative Staff;
- PhD students;
- Research fellows;
- Research assistants;
- Residents;
- Students (students regularly enrolled in institutional study courses. Including: Erasmus students, students enrolled on inter-university courses);
- Collaborators with whom there is a formalised employment or collaboration relationship of any kind on a fixed-term basis;
- Consultants and suppliers;
- Spin-offs and start-ups;
- External companies;
- Guests.

TITLE I
Information Security

1. Classification of information

The University has defined a specific policy, see attached ***Data Classification Policy***.

2. Information Sharing

Data and documents used in work activities must be shared in the manner described in the *Data Classification Policy* document. In particular, data to which a protection level higher than *1-low* is attributed must be saved and stored on the tools designated by the University (e.g.: network folders divided by area or competence and cloud sharing tools).

Removable devices (e.g. USB flash drives and external USB disks) must only be used for business purposes and must be provided by the University (personal media cannot be used). In particular, removable devices containing data that are assigned a protection level higher than *1-low* must implement encryption so that they cannot be read in the event of theft or loss of the media. The media must be stored with the utmost care to prevent theft or loss.

The sharing of data with parties outside the University is only authorised within the scope of work and must follow standards, protocols and channels that provide for encryption. In general, all data exchanges with external parties must take place over encrypted channels to guarantee data confidentiality, i.e. VPN networks, HTTPS/TSL/SFTP connections, etc.

The use of personal sharing services (e.g. Google Drive, DropBox, WeTransfer, etc.) for data processing in the context of work activities.

3. Use of the Internet

Access to and use of the Internet are an integral and fundamental part of the IT tools that the University makes available for the performance of work activities and cannot in general be used for personal purposes.

The Athenaeum identifies the availability and security of network connections as some of the key elements to ensure the efficiency of processes and the safeguarding of data. This implies the need for policies and regulations that encourage responsible use of shared resources, and in particular of the Internet.

The University regulates the traffic allowed in and out of the University network and by means of content filtering technologies (see the attached ***Network Traffic Filtering Policy***) it may prevent or restrict access to services and/or content that it deems to be in its sole discretion:

- offences;
- inappropriate;
- dangerous to the security of data and persons;
- not relevant to the performance of work.

If resources that the user considers necessary for work purposes are also inaccessible, the user may submit a duly justified request to the Information Systems Area (hereinafter ASI) to lift the block temporarily or permanently.

4. Use of e-mail

The University's e-mail profile is a working tool and the user is responsible for its correct use in accordance with the provisions of these regulations and the ***Regulations for the Use of the University's Electronic Mail*** in accordance with current legislation. Use for personal purposes is forbidden. The user is responsible for:

- use the e-mail service only for the institutional purposes of the University;
- not cause damage and/or harm to the University, third parties or other users;
- always be guided by principles of diligence, fairness and good faith, conforming in the content and form of messages to appropriate standards of courtesy and good conduct.

The user may not use e-mail to deliberately send, even via links or attachments in any format (e.g. text, photos, video, audio, etc.), messages that

- may damage the reputation and image of the University or compromise its relations with third parties;
- are defamatory, obscene, pornographic, offensive, likely to cause harm, or may be considered a source of harassment or religious, sexual, racial or political discrimination;
- contain non-institutional, overt, covert advertising or private commercial communications;
- may infringe existing legislation, in particular copyright legislation;
- contain malware or other malicious programmes or act as spam messages unwanted (known as 'spam').

The user is responsible for the correct management of access credentials to the mail profile electronics, as defined in these regulations.

5. Paper documents

All paper documents must be managed in such a way as to minimise the time spent outside the archives or cabinets or containers provided by the operational units. The utmost care must be taken for documents located in premises accessible to the public. Only expressly authorised personnel may access the archives. Archives must be locked, compatibly with service requirements. Copies of documents must be treated, with regard to the protection of personal data contained therein, with the same care as the originals. Users are required to be vigilant against access to their premises by unidentified or unauthorised personnel. All paper documents of an administrative nature containing personal data or data of the University with restricted access must be disposed of using the document shredders provided, subject to an authorisation procedure by the competent superintendence for archival assets as provided for by the reference legislation.

Users should use the printer closest to their workstation whenever possible. Printed documents should not be left unattended to avoid unauthorised access to data, if possible it is better to favour the presence printing option initiated by a personal code. The re-use of printouts as recycling paper is only permitted when the documents contain non-personal and public data, in other cases the copies must be disposed of using the document shredders provided. Retention schedules are governed by the provisions of the Protocol Management Manual and the Manual Selection and Disposal.

6. Controlling, monitoring and recording

The University reserves the right to monitor access, use and operation of the ICT services it provides, either through centralised automatic monitoring systems, or through agents installed on workstations, or during maintenance operations; it also reserves the right to keep activity logs of various types inherent to the services in compliance with current legislation on the processing of personal data (see ***theLog Management Policy*** annexed , which details the sources from which the logs are collected and how they are managed)

These controls are aimed at:

- comply with mandatory data protection and copyright legislation;
- respond to any requests from the judicial authorities;
- ensure the security of services, including through computer intrusion detection systems (IDS);
- verify the proper management of data and information flows;
- implement the inventory of network resources and software used;
- process usage statistics, managing the data in anonymous form, relating to information systems;
- carry out activities related to technical/operational changes;
- verify the correct configuration of the systems;
- collect and preserve forensic evidence to support any legal action involving the University;
- countering improper and/or unlawful use and more generally contrary to the acceptable use policy, these rules and regulations;
- monitor use of exposed credentials.

Any use of the data collected for purposes other than those mentioned above, in particular for any form of remote control of users, is excluded.

Access to activity logs is only allowed to authorised personnel and primarily concerns aggregated data not referable to an individual user. Access to the utilisation data of an individual user, where necessary, takes place for justified reasons. Prolonged and constant monitoring is not permitted under any circumstances.

Some activities (e.g. system administrators) are collected and managed in compliance with current legislation.

7. Security Incident Management

Incidents are tracked in a special register according to the annexed ***Security Incident Management Policy***.

All users are obliged to promptly report any anomaly in the operation of the University's information system or any voluntary or accidental behaviour, even by third parties outside the University, that may expose the data being processed to the risk of theft, loss or unauthorised modification. In the event of a suspected compromise of the IT tools by malware or by a party external to the University, this must be reported as soon as possible to the contacts listed in the annex.

The preventive security measures by the University and the responsible behaviour of employees reduce the likelihood of a security incident occurring, but not the cancel, so it is very important that any abnormal situation is handled in the correct way, also to enable the university to respond to all legal obligations regarding data protection in a timely manner.

A security incident must never be concealed, and it is very important that in the event of a suspected compromise of a work tool or personal access credentials, the user involved follows this simple protocol:

- do not switch off the device (e.g. PC, Smartphone, etc.) for any reason;
- interrupt the data network connection (e.g. disconnect the network cable, disable WIFI. etc.);
- do not delete anything from the device because the data collected can be crucial for the analysis and resolution of the incident;
- Immediately report the anomaly as a potential safety incident and follow the instructions given.

8. Limitation of resource utilisation

Following detection of a cyber incident and/or response to requests from Investigative Authorities and in view of the possibility of having to respond to possible legal obligations to comply with the chain of custody aimed at preserving evidence of particularly serious incidents, ASI may

- restrict or prevent use of the device (e.g. exclusion from the University network) or access to Athenaeum services;
- request delivery of the device for the time needed to perform the analysis activities and resolution of the incident;
- impose the safe and ASI-verified restoration of the device as a condition required for access to University services.

TITLE II
Management and use University devices

1. Computer tools

Computer workstations and, more generally, tools for processing information include devices owned by the University, including those purchased through research funds, assigned to staff, such as, but not limited to

a. desktop personal computer;
b. portable personal computers;
c. thin-client and diskless stations;
d. virtual desktop;
e. tablets and handheld devices;
f. smartphones and landline phones;
g. server;
h. printers.

Each device, when possible, is placed in the University's Active Directory domain (on-premise or cloud), with predefined profiles based on the user's role and task.

2. Management

The workstation must only be used for institutional purposes and only work-related data must be stored on it.

The use of the University's tools must always be based on the principles of correctness and lawfulness; in particular, it is forbidden to modify the hardware and/or software configuration of the IT tools granted for use, by adding or removing components, with respect to the standard defined and provided by the University or by circumventing or compromising protection mechanisms.

It is forbidden:

- maliciously deleting University data or copying them onto personal media;
- acting deliberately to degrade the operability of the University's systems and network and to prevent their use by other users;
- transfer information (e.g. software, data, etc.) and documents concerning intellectual property, except for the performance of its institutional functions;
- install, execute or disseminate on any computer and on the network programmes that may damage systems or lead to unauthorised access to data (e.g. malware, etc.);
- use any kind of computer or electronic system to monitor the activities of other users, to read, copy or delete data of other users;
- use software that jeopardises system security and data protection;
- install software without a valid user licence;
- use University tools for storing or sharing material for which there is a violation of the legislation protecting copyright, as well as pornographic material or material that is in any way unlawful or harmful to human dignity.

Compliance with these requirements contributes to the prevention of computer crime.

If necessary, users may request, after verification by their
responsibleupdating its configuration by contacting ASI.

On termination employment or if the conditions for which users received them no longer exist, including in cases of change of job and/or transfer to another Unit/Area, they must return the IT tools in their possession intact and in good condition.

2.1 Saving data

Workstations within the University domain must store data in the shared disk space made available by the University and managed by ASI (e.g. shared folders, OneDrive, Sharepoint) as it is subject to the appropriate procedures guaranteeing the availability of the data.
For workstations that are temporarily out of the domain, it will be the sole responsibility of the user to make backup copies of the data, taking into account the provisions of current legislation and the *Data Classification Policy*.

2.2 Manning the post

The PC must be switched off every evening before leaving the offices and whenever there is a need to leave the workplace, even when you are on a mission, smart-working, teleworking, etc.) in premises outside the University, password protection must be activated (screen saver with password or computer lock with password). Leaving a computer unattended and connected to the network may lead to its use by third parties without there being any possibility of subsequently proving undue use.

2.3 Security Tools

All fixed and mobile personal computers are equipped with tools to automatically update operating systems, protect against malware and monitor anomalies: the user must not in any way hinder or inhibit the operation of these tools, simply report any type of problem to the IT helpdesk in good time.
The University can make use of centralised management systems for fixed and mobile personal computers in order to

- activate additional authentication procedures;
- enforce adherence to pre-established configurations and inhibit their modification;
- automatically inventory hardware and software;
- define adequate data back-up policies;
- automatically update operating systems and software;
- activate remote wiping procedures to be used in case of loss/stolen device;
- automatically encrypt the data;
- inhibit the installation of unwanted applications;
- filter incoming content to the University's network, inhibiting in advance any content deemed inappropriate or unnecessary for the performance of work activities.

Each instrument provided by the University can also be equipped with remote management and monitoring software. ASI personnel use these tools to connect to individual workstations order to guarantee technical support. Remote intervention is only carried out on user call or following the detection of technical problems. In the latter case, notification of the need for intervention will be given to the user, who must explicitly authorise the support staff to carry out the activity.

2.4 Theft or loss

Laptops must be stored in a way that minimises the risk of theft and loss, especially when outside the university. Laptop storage media are encrypted so that no one can gain unauthorised access to the data even if they come into physical possession of the devices. This generally requires the user to enter an unlock code provided by the University when starting up the PC, which must remain secret and must be managed according to the access credentials guidelines defined in these regulations.

In the event of theft or loss of any device (fixed or mobile), users are required to

- notify the IT helpdesk of the incident, at the same time requesting the blocking of the profiles or SIM card if applicable and, if the device contains personal data, also write to the databreach communication address (attached contact details);
- file a complaint with the police;
- request a new endowment from ASI by attaching the complaint made to the police.

3. Use of tools not provided by the University within the University premises

Regarding the use of tools not provided by the University (even just connecting to the University network is a use):

- is allowed to connect to the University WiFi network via authenticated access with University credentials;
- it is permitted to connect to the wired network according to the provisions of TITLE III Art. Connection of devices to the network.

4. Teleworking or agile working

Teleworking and agile working (smart-working) are carried out only with proprietary devices of the University that comply with the guidelines and security measures set out in these Regulations.

The preceding chapter does not apply in emergency situations duly codified by legal provisions.

4.1. Protection against theft and loss of data on devices

Given that the working environment not the usual office environment and that there may be greater opportunities for unauthorised access to data by parties outside the University, all the provisions described in these regulations apply without exception (see especially Section 2).

4.2. Protection of data in transit over the network

All work-related communications must take place on encrypted communication channels, which therefore use appropriate protocols to guarantee data confidentiality. The University defines and informs those concerned which tools are suitable for the purposes of data exchange, videoconferencing, etc.. The indications provided by the University are binding and it is therefore forbidden to use other tools that may not have the required security standards.

Remote access to the University network is guaranteed through the use of an encrypted VPN (Virtual Private Network) communication channel, which is activated through use of specific software (VPN client) installed on enabled devices. The user will use personal access credentials to be managed according to the provisions of these regulations. The University may modify the technical connection modalities favouring other equivalent solutions from a security point of view such as the use of virtual desktops provided by the University.

If the connection to the Internet is made via the user's private WiFi network (e.g. home connection), the user must ensure that the network's security level is compatible with the University's requirements by following these guidelines, for example:

- change the default password for WIFI access;
- Disable, when possibleadministrative access to the WiFi router from an external network;
- verify that the University's PC does not share resources with any other device on the home network;
- prevent the University PC from accessing other storage devices on the home network (NAS, external disks, etc.).

In the event that public networks are used (e.g. hotel WiFi, airport, libraries, etc.), it is essential to use VPN to access University services that authentication. VPN connections are monitored for security and regulatory compliance reasons, particularly in relation to privileged profile access. All system monitoring and control modes, as well as remote assistance are also active in smart working.

5. Assistance

Assistance is provided in accordance with Area Service Catalogue
Information Systems.

6. Smartphones and Tablets

If a mobile phone/smartphone/tablet is assigned by the University to the user, latter shall be responsible for its safekeeping and proper use. In addition to the use of the usual work tools (e.g.: e-mail, document management, etc.), the smartphone may be configured by the University as a code generator for access to systems or applications that require two-factor authentication, therefore it plays a central role in information security management strategies and must be adequately protected.

The storage media of mobile devices are encrypted and each device will be delivered with unlocking code (PIN) to protect it from unauthorised access in the event of theft or loss: the PIN code cannot be removed for any reason.

The University may make use of centralised management systems for mobile devices as already defined in TITLE II Article 2.3 Security tools for fixed and mobile workstations.

Any specific rules for the use of mobile devices may be made explicit in the forms for assigning the devices to users. The University is in any case not liable for the loss of user data and personal documents stored on the device.

TITLE III
ATHENAEUM NETWORK

1. Access

The University of Parma considers the University Data Network a strategic and fundamental element for the pursuit of its institutional aims and, therefore, promotes its development, proper functioning and security. It therefore encourages users (lecturers, PTA, students, ...) to access it with the available technologies, according to differentiated profiles, while adopting all the necessary measures to mitigate risk.

The access service to the internal network and to the Internet must be used for institutional purposes, in compliance with the rules of conduct laid down in these regulations and with the GARR Consortium's Use Policy). AUP (Acceptable The regulations, in particular, are to be considered always applicable regardless of the type of device used to access the University network.

In order to control and manage the security of the University's network, access to the wired network may take place by requesting credentials and restrictions may be applied to browsing (e.g. blocking URLs that lead to dangerous or malicious content).

2. Connecting devices

For the first connection of any device to the network, a request must be made via the IT helpdesk to the ASI, which will issue the necessary information (e.g. IP Address, Gateway, Netmask, DNS, ...) according to the authorisation criteria in force.

The device, therefore, is inventoried as an 'active resource' and the IP address/MAC ADDRESS pair is registered and associated to the user who requested it (whether the address is static or dynamically provided, e.g. with DHCP).

In order to manage the security of the device and the University's network, the ASI will install low-impact software agents that will centrally provide information on the vulnerabilities present on the device, the presence of malicious, unauthorised software or other technical information useful for managing the University's security system.

These agents do not collect data for purpose of monitoring user activity and must not be removed or deactivated.

3. Connection of computer labs and public workstations

1. The connection of computer laboratory workstations, public workstations or other types of equipped areas to the University network is via the virtualisation infrastructure of the University desktops
2. Within the facilities referred to in point 1, it is forbidden to disconnect devices from the wired network and/or connect devices other than those installed and authorised by the University to the wired network.

4. Requests for allocation of externally accessible resources and services

For institutional purposes (compatible with GARR's AUPs), anyone may request the allocation of adequate resources and communication services over defined IPs by making an explicit and adequately motivated request that will be assessed and, if necessary, approved by the Rector or his delegate.

Requests to open communication ports/protocols will be evaluated against security criteria in order to minimise risk.

Assignees are responsible for keeping their systems and applications up-to-date and correctly configured so as not to pose a risk to information security and must comply with ASI's instructions regarding any configuration and installation of tools required for security checks (e.g.: agents, probes ...).

In this regard, ASI carries out periodic checks on vulnerabilities and reports criticalities that must be corrected within the agreed timeframe, or else privileges will be forfeited and the assigned services will be blocked.

ASI also has the power to monitor the network, systems, services and applications in order to highlight anomalies and security incidents that will be handled according to the policies in force.

The management of incoming and outgoing traffic from the University network involves the implicit denial of any communication flow to and from the outside that is not explicitly authorised. This makes it possible to control both the subjects that can communicate with the outside world and the services that the University network exposes to the public Internet or to partners, suppliers, service users, researchers, etc.

Systems offering services to external public or private networks must be installed on dedicated and centrally managed infrastructures, thus facilitating the management of network security and the adequacy of controls applied to systems and applications.

TITLE IV
User profiling

1. University Digital Identity

A digital identity consists of the information about a user, called attributes, used to represent his or her identity, status, legal form or other special characteristics and is verified through a computerised identification and authentication system.

The University's digital identities consist of user names, passwords personal data, career information and other data for the exclusive use of IT systems and procedures. The digital identity is instrumental in accessing one or more telematic services.

The University encourages participation in the Authentication Federations provided for by national legislation (SPID) or in use on university and research networks at national, European and global level, such as Eduroam and IDEM, which operate in a federated identity logic.

2. Holders of digital identities

The holders of the University's digital identities are all those who need to use a service of the university itself.

3. Responsibilities of digital identity holders

1. Each digital identity holder, when using the services, must not:
   - Violating the privacy of other Users or the integrity of data not pertaining to it, whether personal or not;
   - Compromising the integrity of systems or services;
   - Consuming resources to such an extent that the efficiency of other services is compromised;
   - Committing, facilitating or indirectly supporting acts of cybercrime against and/or through the University's infrastructure and resources;
   - Exploiting the University'services to gain unauthorised access to University resources or of third parties;
   - Sharing access to University services unauthorised third parties;
   - Using false identitiesanonymity or using resources that allow even partial anonymity;
   - Breach the obligations contractually undertaken by the University for the implementation and management of the Internal Network, in particular by transferring and making available material in breach of the legislation in force and, in particular, the rules on intellectual property, software licences and the regulations of network connectivity providers (GARR);
   - Carrying out activities that cause malfunctioning, diminish regular operations, distract resources (people, capacity, processing power), damage or restrict the usability of services and resources;
   - Breach the security of archives and databases, make unauthorised transfers of information (e.g. software, databases, etc.), intercept, attempt to intercept or access data in transit on the Network, of which one is not the specific recipient;
   - Committing or attempting to commit the following actions: destroying, intercepting, gaining unauthorised access to the data of other users or third parties, using, intercepting or disseminating passwords or access codes or cryptographic keys of other users or third parties, and in general committing activities that violate the confidentiality of other users or third parties, as protected by applicable civil, criminal and administrative laws;

- connecting equipment to network infrastructure without ASI authorisation, including personal devices;
- create or disseminate potentially offensive, defamatory or obscene images, data or other material;
- engage in activities that damage the image and good name of the University;
- use the University's IT services and resources for commercial purposes and for political or electoral propaganda, except in specifically authorised cases.

2. IT services and resources provided in collaboration with parties outside the University are subject to terms and conditions of service established with the relevant providers. If a service is used in collaboration with external companies, the user accepts the terms use when accessing the service. The Athenaeum makes references to the terms and conditions of service available in Annex A of these regulations or when accessing the service for the first time.

4. Profile credentials lifecycle

Access credentials for each profile are created, deactivated, suspended and deleted for the different user categories according to the schemes contained in the annex ***Digital Identity Lifecycle***.

5. Authentication

The authentication methods required to use the services are set out in the Service Catalogue (hereinafter referred to as the CS). A distinction is made between services that do not require authentication, services accessible via Centralised Authentication Credentials and services accessible via service-specific credentials.
According to the provisions of Article 64 of the CAD, access to the University's services must be allowed through the use of SPID credentials.

6. Centralised Authentication Credentials

The Centralised Authentication Credentials (ref. § 2.5 of the CoS) are the main authentication system for the University's IT services. Credentials consist of an identifier (also called username or user id) and a password. The identifier generally coincides with the user's university email address, but for some categories of users it can be represented by a numeric code or be enhanced with the user's private email address. The identifier may be modified during the user's relationship with the University (e.g. change from student to employee), but a unique relationship is maintained between the Centralised Authentication Credentials and user's digital identity in the University's information system.

6.1. Password Policy

The password must meet the robustness and security criteria set out in the attached *Password* .*Policy*

6.2. Issue, suspension and revocation of credentials

Credentials, depending on the user's category, are issued ex officio or upon registration. Credentials may be suspended, e.g. for security reasons in the event of a suspected compromise.

6.3. Rules for the use of credentials

Credentials are strictly personal, the user is obliged to keep them diligently, taking care that they are not misused. Transferring one's credentials to third parties constitutes a violation of these rules.

Outside the services included in single sign-on management, the user must choose different passwords for each system or application which they have access, including any third-party services to which they must register with an e-mail profile provided by the University. Credentials must never be reused.

The University may determine that access to certain data entails a higher risk and therefore requires a higher level of security: in this case, the use of two- or multi-factor authentication systems involving the entry of a temporary code generated by a mobile application or dedicated device may be mandatory. Operational instructions for proper use will be provided to the users concerned.

All credentials are strictly personal and each user is responsible for their safekeeping and confidentiality. University policies require periodic expiry of access credentials; the user will be automatically notified of the need to choose a new password, always respecting the previously defined criteria.

If it is not possible to implement an automatic password change procedure for certain systems or applications, the university will define a manual procedure to be referred to.

If you suspect that your password has lost its secrecy characteristic, you must immediately change it and notify the IT helpdesk. Similarly, if the user becomes aware of another user's hacked credentials, he or she must notify the IT helpdesk immediately in the same manner.

7. Local credentials

For services that cannot be integrated into the centralised authentication system, the use of local credentials issued by the structure in charge of providing the service is envisaged.

In the case of credential systems based on identification code and password, the *password Password Policy*.must be managed with criteria aligned with the

8. Enabling the use of services

The use of services requiring authentication is conditional not only on the possession of authentication credentials, but also on their authorisation for the service in question. The University adopts an enabling policy based on roles and access profiles: several access profiles are identified for each service, one or more access profiles are assigned to each role for the various services, and each user is assigned to one or more roles.

Each user is associated with at least one basic role corresponding to the category to which he or she belongs and, possibly, with additional roles based mainly on the user's category, the structure to which he or she belongs and the activities for which he or she is responsible.

The membership criteria for the additional roles and the access profiles to be associated to the various roles are established by the management areas and departments through their appointees, in coordination with the personnel in charge of the operational management of the entitlement systems, who shall be responsible, inter alia, for maintaining a catalogue of existing roles and access profiles and for periodically verifying the correct association of users to the roles and access profiles corresponding to

each role. Verification is carried out more punctually and frequently for roles that allow access to sensitive and/or confidential information.
The association with a role may be made ex officio or on the basis of a request made by the user himself or by a responsible person (e.g. the head of the relevant structure or the teacher in charge), as the case may be.
For reasons of security and confidentiality:

- authorisations to use services are strictly personal, it is prohibited to use one's own authorisations to allow other users or third parties to use the services with one's own access privileges;
- Each role is assigned the minimum access profiles required to perform the activities of the users assigned to that role;
- it is the responsibility of users to promptly report any errors in the allocation of privileges to enable managers;
- privileges may be temporarily suspended, after notice to the users concerned, in the event of abuse in the use of the services or for other justified technical or other needs;
- Roles are revoked from the user when the conditions for which the role was assigned are no longer in place.

The assignment of a role entails the simultaneous activation of the access privileges provided for that role on the various services, and the revocation of a role entails the removal of access privileges. For some services it is provided that access privileges are not revoked immediately, but after a predefined period of time indicated in the CS or in the Digital Identity Lifecycle Annex these regulations or in a specific article of any service-specific regulation.

Annexes and references

Section A - Terms and conditions of third-party services

- GARR - acceptable use policy AUP

Section B (contacts)

HELPDESK IT
Email: helpdesk.informatico@unipr.it
Telephone: +39.0521.90.6789

DATA BREACH NOTIFICATION
Emaildatabreach@unipr.it

DATA PROTECTION OFFICER
Emaildpo@unipr.it

Section C - University Policies and Procedures

1. Data Classification Policy
2. Network Traffic Filtering Policy
3. Log Management Policy
4. Password Policy
5. Security Incident Management Policy
6. Digital Identity Lifecycle
7. Rules for the Use of the University Electronic Mail
8. Code of Ethics
9. Catalogue of IT services