APPENDIX 4: INFORMATION TECHNOLOGY CHARTER

(Approved by the Board of Directors on March 12, 2026 – Annex to the Internal Regulations)

1. Preamble

This document sets forth the rules governing the use of equipment, systems, software, and computer networks (hereinafter referred to as "digital resources or services") of the National Institute of Applied Sciences of Toulouse (INSA).

A "User" shall mean any individual making use of INSA's digital resources or services, including, but not limited to, students, staff members, guests, and volunteer collaborators.

This Charter defines the rights, duties, and obligations of Users in order to ensure the proper and fair use of information technology resources, in compliance with applicable laws and with due respect for others.

This Charter is annexed to the Internal rules of INSA and forms an integral and inseparable part thereof. It shall enter into force on March 12, 2026, and shall supersede all prior documents or charters relating to the use of INSA's information systems.

INSA reserves the right to amend this Charter in order to comply with legal, regulatory, or case law developments, changes in the use of information technology resources, or for any other reason deemed appropriate. In the event of such amendments, INSA shall specify the effective date of the revised version.

2. Commitments of INSA Toulouse

The Digital Services Center (CSN), within the limits of its resources and operational constraints, undertakes to:

- Provide Users with equipment and software appropriate to their needs;
- Grant access to the INSA network and, through it, to the Internet, via an IT account and, where applicable, an email address;
- Maintain and secure, to the best of its ability, the IT infrastructure, networks, and data;
- Ensure continuity of the services provided.

Mandatory maintenance operations may be scheduled by the CSN in order to update digital services, which may result in temporary service disruptions. Users shall be informed in advance of such maintenance operations.

3. User Obligations

IT Account

The CSN shall assign each User an IT account consisting of a username and password granting access to digital resources and services. Such credentials are strictly personal and non-transferable under any circumstances. They must not be reused on any digital service other than those provided by INSA.

Users are responsible for maintaining the security of their accounts. They shall ensure that their passwords are sufficiently robust and shall promptly change them in the event of disclosure or compromise.

Proper Use of Resources

The use of digital resources and services (including wired networks, Wi-Fi, applications, managed cloud services, and workstations provided by the CSN) is strictly reserved for activities related to teaching, research, and the operational needs of INSA.

However, limited personal use is tolerated, provided that such use remains reasonable and proportionate, does not interfere with professional duties, and does not adversely affect the proper functioning of INSA's digital resources or its reputation. Any additional costs resulting from residual personal use must remain negligible in relation to the overall operating costs.

Compliance with Legal and Security Requirements

Users shall comply with all applicable laws and regulations governing the use of information and communication technologies, including, but not limited to, those relating to:

- Violations of privacy;
- Defamatory or abusive statements;
- cybercrime;
- Unauthorized access to, or maintenance within, data processing systems;
- Infringement of intellectual property rights and image rights.

Users shall act in a responsible and prudent manner, in particular by ensuring the protection of their workstations and INSA's digital services. Users shall not bypass or attempt to bypass any security warnings or mechanisms. In case of doubt, Users shall seek guidance from the CSN prior to performing any action.

Particular caution shall be exercised when opening documents, links, or applications originating from unknown sources (e.g., emails or USB devices).

The use of INSA credentials (username and password) on untrusted devices (such as public computers) or on websites not affiliated with INSA, or of doubtful authenticity or purpose, is strictly prohibited.

Users shall comply with all instructions issued by the CSN (including, for example, system and antivirus updates) and shall report any incident, suspected breach, or malfunction without delay.

Users shall respect INSA equipment and shall not alter its configuration (systems or software) without the prior authorization of the CSN.

Equipment

All equipment provided (including computers, monitors, smartphones, and external devices) professional duties remains INSA property and must be returned upon termination of the User's association with INSA, in accordance with applicable departure procedures.

Users are responsible for deleting all personal data prior to returning such equipment. Upon return, all data contained on the equipment shall be presumed to be exclusively professional in nature.

Users are responsible for the safekeeping of their equipment and shall exercise particular vigilance when traveling outside the workplace.

When traveling abroad on assignment, Users may, depending on the destination country, be required to use a sanitized device instead of their usual workstation. Users shall comply with INSA's recommendations in this regard and shall consult the CSN in case of doubt.

Cyber Hygiene

Users shall ensure the proper maintenance of their workstations and shall keep them up to date and secure by promptly carrying out any required updates.

Users are responsible for the documents they handle and shall ensure that access is restricted to authorized persons. Documents related to INSA activities shall be organized, classified, and backed up in shared spaces.

In order to reduce INSA's digital footprint, Users shall pay particular attention to obsolete data and to personal data storage unrelated to INSA activities, which shall remain minimal. Such data shall be deleted or stored in a designated "private" folder.

Users working on devices not managed by the CSN (including personal devices or devices provided by another institution) and handling professional data shall minimize data persistence and prioritize storage on INSA-provided resources.

Users shall ensure that their physical workspace does not expose sensitive information. Passwords shall not be displayed, and sensitive documents shall not be left unattended. Workspaces shall be secured when unattended, where possible.

4. User Data

All data (including files, emails, and web publications) stored on INSA digital resources or services, or produced in the course of teaching, research, or institutional operations, including on equipment not owned by INSA (e.g., SaaS platforms), shall be deemed professional in nature and shall be the property of INSA, unless explicitly stated otherwise.

Data clearly identified as "PRIVATE" or "private," or any equivalent designation indicating the User's intention to restrict access, shall be considered personal.

Publications made via INSA servers are inherently professional in nature.

Upon departure, professional data must be made available to the Director of INSA (for academic staff) or to the relevant line manager (for other Users). Failing this, such data may be transmitted by a CSN administrator upon request.

Student data of a professional nature may be made available to teaching staff by a CSN administrator upon request to ensure continuity of instruction.

In the event of a breach of these rules or in emergency situations necessary to preserve systems and data, the CSN may access the content of User files. Administrators shall, in all cases, respect the confidentiality of any information accessed.

Sensitive Data

Data shall be considered “sensitive” where it relates to contracts, patents, or strategic or financial information regarding INSA. The classification of sensitive data is defined in INSA’s data classification framework.

Data containing personal information—i.e., any information that allows, directly or indirectly, the identification of natural persons—shall also be considered sensitive and must be declared to the Data Protection Officer (DPO) (contact-dpo@insa-toulouse.fr).

All operations involving sensitive data (creation, modification, storage, archiving) shall be carried out exclusively on equipment or services authorized and operated by the CSN. The storage of such data on unauthorized systems or services is strictly prohibited.

Backup

All User data stored on digital resources or services shall be subject to backup procedures, irrespective of directory, file, or message names (including those marked as private), in order to ensure availability in the event of an incident.

On portable devices (laptops), only the “NoBackup” directory is excluded from backup, allowing Users to store files they do not wish to be backed up.

Retention

Upon a User’s departure, data stored in their personal workspace (home directory), as well as email messages, shall be retained for a period of two (2) years following account closure, after which they shall be deleted.

Data stored in shared spaces or shared mailboxes shall be retained insofar as necessary to ensure continuity of operations.

Email

Users shall be assigned one or more institutional email addresses upon arrival at INSA, where necessary for the performance of their duties. Such addresses may be automatically subscribed to institutional mailing lists, without the possibility for Users to opt out.

Reasonable and occasional personal use of email is permitted, provided that it does not interfere with the normal flow of institutional communications.

All emails sent, received, or stored via INSA digital resources shall be presumed to be professional in nature unless clearly identified as “PRIVATE” or “private.”

If a User receives a message in error, any use, copying, or dissemination, in whole or in part, is strictly prohibited. The User must delete the message and inform the sender immediately.

Users are strongly encouraged to use only INSA-provided tools (e.g., webmail) for email access and transmission. The forwarding of emails to external servers is strongly discouraged.

Email communications on INSA servers are subject to security measures, including spam filtering, antivirus protection, restrictions on attachment types and sizes, and verification of senders.

In the event of a data security incident, the CSN may take necessary precautionary measures, including the deletion of messages.

5. Security Measures

INSA has implemented technical measures to monitor, audit, and secure digital resources and services. The CSN may take action, including suspension of network access, in the event of detection of suspicious behavior by a User or a device.

Any attempt to circumvent or bypass such security measures is strictly prohibited.

Internet Access

Access to the Internet is authorized solely for professional purposes (administrative or educational).

Filtering mechanisms have been implemented to protect digital resources and services from malicious or harmful content.

Reasonable personal use of Internet services is tolerated, provided that it does not affect the performance of INSA's digital services.

Access to content likely to generate significant consumption of network resources may be restricted.

As INSA's network is connected to the Internet via the national Renater network, Users shall comply with the Renater charters, whether connected via wired or wireless access:

- https://www.renater.fr/wp-content/uploads/2022/01/charte-de-bon-usage-de-linformatique-et-du-reseau-renater.pdf
- https://www.renater.fr/wp-content/uploads/2022/01/charte-deontologique-renater-fr.pdf

6. Departure

Upon termination of their association with INSA, Users shall delete all personal data from their workstations and shared storage spaces and shall return all equipment in their possession to the CSN, including equipment provided for remote work.

Users are advised to unsubscribe from mailing lists and to notify the relevant services, departments, laboratories, and centers with which they have interacted.

7. Traceability

For the purposes of judicial investigations, security, maintenance, and technical management, connection data enabling identification of the workstation or User, as well as activity logs, shall be retained for the duration recommended by the French Data Protection Authority (CNIL).

Such data may include volumes of data exchanged, identification of websites accessed, and email routing information, without recording the content of communications.

8. Sanctions

In the event of non-compliance with the provisions set forth herein, Users may be temporarily denied access to IT resources by the CSN, following adversarial proceedings or in cases of force majeure. Users may appeal such decisions to the Director of INSA.

Disciplinary sanctions applicable within higher education institutions may also apply.

Civil and criminal sanctions, as provided for under applicable laws, may likewise be imposed.