IT Policies and guidelines for the use and management of Digital resources of the University of Technology of Troyes (UTT)

Table of contents

Acronyms

Notation	Description	Page List
BD	Board of Directors (Conseil d'Administration)	3–21
CAD	Computer Aided Design	11
CISO	Chief Information Security Officer (RSSI) rssi@utt.fr	6, 9, 13
DNum	Digital Department (Direction du Numérique)	7, 11
DPO	Data Protection Officer dpo@utt.fr	5, 15
DW	Digital Workplace (Environnement Numérique de Travail)	11, 19
EC	Executive Committee (Comité de Direction)	3–21
GDPR	General Data Protection Regulation	5, 9, 13
HRD	Human Resources Department (Direction des Ressources Humaines)	7
IS	Information System (Système d'information)	5
IT	Information Technology (informatique)	4
SC	Social Committee (Comité Social d'Administration)	3–21
ScAB	Scientific Advisory Board (Conseil scientifique)	3–21
SSD	Solid State Drive	4
StAB	Studies Advisory Board (Conseil des Études)	3–21
USB	Universal Serial Bus	4
UTT	University of technology of Troyes	4
VAT	Value Added Tax (TVA)	8
VPN	Virtual Private Network	13, 19

Preamble

The purpose of these policies for the use of University of technology of Troyes (UTT)'s IT resources ("Information Technology (informatique) (IT) policies and guidelines") is to define the terms and conditions:

- access to and use of the UTT information system,
- the use and management of Information Technology (informatique) resources in the context of on-site or remote use, in particular remote office.

This document describes the rights and duties of users in compliance with french and international regulations.

1 Scope

The policies consist of general rules that all users must comply with if they want to be able to access:

- UTT IT devices (workstations, servers, software, smartphones and landline phones),
- the UTT computer network (local area network, wired internet network and wifi) from computer devices (eg: workstation, smartphone, tablets), whether personal or not, photocopiers and printers, 3G/4G/5G keys, mass storage devices (USB keys, portable SSD),
- any IT resources lent by the UTT,
- the UTT information system.

The *users* of the UTT's information system and IT resources are:

- students,
- teachers, researchers, teacher-researchers, individual lecturers, associate researchers,
- administrative and technical staff,
- temporary guests (trainees, guests external speakers, members of external juries, etc.),

- associations hosted at UTT,
- more generally, any person who has received authorization from the UTT’s-Information System (Système d’information) (IS)

2 General principles

2.1 Compliance with ethical rules

Uses contrary to the laws and regulations in force and in particular those having as their object or effect the dissemination of political, racist, anti-Semitic, homophobic, sexist ideologies and all forms of incitement to hatred shall be strictly prohibited. Users shall refrain from any defamation, public insult, harassment or objectionable comments.

2.2 Respect for privacy

In accordance with Article 9 of the french ‘Civil Code’, ‘everyone has the right to respect for his or her private life.’ As such, no image or information relating to the private life of another person may be posted online without the consent of the person concerned.

2.3 Protection of personal data

The UTT has appointed a Data Protection Officer dpo@utt.fr (DPO). The latter’s mission is to ensure compliance with the provisions of the General Data Protection Regulation (GDPR) and Act No. 78-17 of 6 January 1978, as amended. To carry out their tasks, users can enquire by email at: dpo@utt.fr. Any creation or transmission of files containing personal information outside the university is subject to the authorization of the DPO. For the use of personal data or applications dealing with personal data, users and administrators of the UTT undertake to comply scrupulously with the principles of the regulations in force(confidentiality, minimization, security, etc). Two policies on the protection of personal data supplement the information on the UTT’s commitments on this subject and are intended for staff, students (and candidates) respectively. They are intended to provide information on the rights and obligations of those members of the public and to satisfy the UTT’s obligation to inform them in the context of the processing of their personal data. These policies can be consulted in the UTT documents under the title ‘UTT Personal Data Protection Guidelines’ (one document is dedicated to students, the other to staff).

2.4 Information system security

The University of Technology of Troyes attaches paramount importance to the security of its IT systems. To guarantee this security, the UTT has set up a dedicated team composed of the Chief Information Security Officer (RSSI) rssi@utt.fr (CISO) and several alternates, all responsible for supervising and coordinating the implementation of IT security measures, in strict compliance with current standards and regulations. Given the increasing complexity of IT threats, it is crucial that each member of the academic community actively participates in safeguarding the security of UTT's IT systems. Thus, in the event of the discovery of a security breach, an intrusion attempt or any other incident related to IT security, it is imperative that users immediately report these incidents to the CISO. To facilitate this, a dedicated e-mail address has been set up: rssi@utt.fr.

2.5 Filtering

The UTT may filter or prohibit access to certain categories of sites which are illegal or present a proven threat to the security of its information system, - after informing the Social Committee (Comité Social d'Administration) (SC). In this case, the list of these categories of sites is disseminated to users.

2.6 IT log management policy

UTT has a log management policy in place for all the digital tools and services it makes available to users. The legal retention period for log files is one year from the date of registration. The UTT shall refrain from exploiting them for more than three months unless requested by a court or in an anonymized form.

2.7 Intellectual property

The use of digital means implies respect for intellectual property rights, in particular the copyright and those of its owners and, more generally, of all third parties holding such rights. In particular, each user must first check the conditions of use and comply with them.

2.8 Use of digital and material means

The digital and material resources made available to users by the UTT are made available for professional use. For the purposes of these policies, the use of these means is of a professional nature where it occurs:

- in the context of the tasks entrusted by the UTT, for users who are members of its staff: teachers, administrative or technical staff, but also its service providers and partners,

- as part of educational activities, for its student users.

Therefore, the use for private purposes must be punctual, non-profit and reasonable. It must not impair the proper functioning of UTT's IT resources. The use of UTT computer equipment is strictly personal and its use by a third party, particularly in the family setting, is prohibited. The installation of software for purely non-professional purposes is prohibited. Computer workstations made available to staff and doctoral students for their work, or to any user within the framework of a project, shall be managed in accordance with the rules laid down in this document.

2.9 Return of computer equipment

All the IT equipment lent and/or made available by the Digital Department (Direction du Numérique) (DNum) must be returned on the last day of presence at the UTT, at the end of the contract or activity or projects, put on standby, decommissioning,transfer. For people with long-term work stoppages, the administration reserves the right to ask for the equipment to be returned. All mobile equipment must be returned to the DNum's Support and Computer Park Management Unit. Any exception to this rule must be duly notified to the Human Resources Department (Direction des Ressources Humaines) (HRD) by the line manager or project manager, with an indication of the duration of the exception. This exception will be sent to the DNum after validation.

The basic IT equipment concerns: the PC, the charger, the carrying bag and the docking station. Any loan of computer equipment shall be the subject of an inventory sheet containing the loaned goods returned in duplicate to the DNum and the user. This list will serve as a reference for the list of goods to be returned. The user must be aware that the non-professional data is deleted before the return. All data present will be deleted by the DNum. Under no circumstances may the equipment made available to the user be the subject of a loan without the prior agreement of the DNum. Except in the case of a donation, in accordance with the procedure for removal from the inventory set out by the accounting agency 'UTT – Procedure for removal of goods', IT equipment not returned at the end of this period will be invoiced, by decision of the authorizing officer as follows:

Computer equipment,telephony, aged strictly*less than 2 ans*	Invoicing in case of non-return	80% of the purchase price
Computer equipment, telephony, aged*more than two years and less than 5 years*	Invoicing in case of non-return	60% of the purchase price
Computer equipment, telephony, aged strictly *more than 5 years*	Invoicing in case of non-return	50% of the purchase price

The purchase price is the cost of purchasing the equipment made available, including Value Added Tax (TVA) (VAT), by the UTT.

The calculated amount re-billed will be rounded down to the nearest euro.

Example of re-invoicing of non-returned "Calculation" configuration equipment, with an initial purchase price by the UTT of EUR 1301.16 inclusive of VAT.

Table 2: Example of re-billing for an acquisition cost of 1301.16€.

Computer equipment strictly less than 2 years old	Invoicing in the event of non-returned	1040€
Computer equipment from 2 years to 5 years old	Invoicing in the event of no-returned	780€
Computer equipment more than 5 years strictly old	Invoicing in the event of no-returned	650€

2.10 Compliance with the rules of computer ethics

It is prohibited to:

- masking one's true identity;
- impersonate another user's account;
- use another user's account and password;
- access information belonging to other network users or to UTT without their agreement;

- alter, modify, delete or modify access rights to accounts belonging to other users of the network or to UTT without their agreement;
- adversely affect the integrity or sensitivity of another user by means of provocative messages, texts or images;
- interrupt or disrupt the normal operation of the network or of a system personal to the network;
- modify or destroy information related to the management of IT infrastructure and systems;
- install software intended to intercept information frames issued on the network to other persons without first informing the Chief Information Security Officer (RSSI) rssi@utt.fr (CISO); finding such software on a machine outside a research or teaching program recognized by the CISO indicates an attempt at illegal, reprehensible and punishable action;
- use on the UTT network encryption means that do not comply with the regulations on cryptology;
- mining cryptocurrencies;
- connect or try to connect to a website (hosted or external) without permission;
- degrade UTT equipment.

3 Provision of computer hardware and software

The role of the DNum is to provide assistance, advice, information and guide choices.

3.1 General purchase and maintenance rules

Purchases of IT equipment are made on budgets managed by the UTT or by third parties under agreement. When projects, requests for funding, including requests for IT equipment or software are prepared, consultation of the DNum prior to submission ensures technical compatibility and compliance with the general policy (resource management, markets, responsible digital, security, GDPR).

The DNum covers expenditure on equipment,renewal and maintenance of the workstations of administrative and technical staff of the administrative organization defined in the organization chart of the UTT.

he DNum covers the costs of equipping, renewing and maintaining the individual workstations of teachers, teachers-researchers and researchers.

The DNum covers expenditure on equipment, renewal and maintenance of self-service IT equipment and training (teaching rooms, practical work rooms, library, laboratories, data center).

Trainees access workstations in self-service computer rooms.

All orders for computer equipment are referred to beforehand and systematically by the DNum in order to verify that it complies with the standards in force at the UTT. The Management and Financial Affairs Department and the DNum check whether it is covered by a public contract.

The entire computer park is administered by the DNum and inventoried. IT equipment purchased by the UTT and hosted outside under agreements is recorded in the UTT inventory. The deliveries are received by UTT and sent externally after signing a loan agreement with the secretariat of the DNum. Computer stations loaned to staff and students are handled by the DNum. The DNum provides a configuration station adapted to the needs of the doctoral students. These equipments can be financed by contract or accompaniment, as part of the thesis contract and their order must be anticipated. The DNum administers and ensures the maintenance of these posts, as well as their reassignment at the end of the thesis work.

3.2 Uniqueness of the workstation

The DNum is responsible for the administration and maintenance of a single individual workstation, connected to the UTT network, for reasons of digital responsibility. An agreement of the management of the UTT, after technical advice from the DNum, is required for any request for an additional post, its maintenance and renewal. Additional equipment can be loaned by the DNum for specific needs (portables, tablets, smartphone.... This equipment must be included in the budget if it is not available at the DNum.

As part of the teleworking protocol, the DNum provides users with: a portable PC, a home kit including an external screen, a keyboard and a wired mouse. Additional equipment may be provided according to the needs of the service and after consultation with the DNum.

3.3 Typical hardware configuration

A catalog of IT services, updated on the Digital Workplace (Environnement Numérique de Travail) (DW), offers standard configurations and associated rates for office automation, calculation and Computer Aided Design (CAD).

3.4 Choice of non-standard IT equipment

In the event that a user wishes equipment outside the standard specifications, a specific and reasoned request must be sent to the DNum, in order to verify the conformity of the product and its integration into the UTT's computer park. It will have to find financing for the additional cost. The DNum will ensure the possible reallocation of the equipment and the conditions of warranty and support. For reasons of responsible digital technology, the DNum advocates the use of personal workstations as terminals, in particular to have computing resources made available by the UTT and its partners.

3.5 Printers, photocopiers and scanners

The use of photocopiers (color and black and white) from the UTT is preferred for printing and scanning documents (scans). Indeed, the financial and environmental costs are lower on this equipment compared to individual printers. The purchase or renewal of primary equipments, the purchase of consumables must meet specific, motivated needs and be provided for on a budget line. The purchase of non-public market equipment must be exceptional and motivated. For responsible digital technology, the recommended period for the use of IT equipment is seven years. The material is renewed if it is no longer suitable for use and if it is sustainable, after consulting the Digital Department (Direction du Numérique) (DNum).

3.6 Computer hardware warranty

Under the public market contract for the purchase of IT equipment, the standard guarantee is five years. In order to be digitally responsible, the Digital Department (Direction du Numérique) (DNum) recommends moving to the extension of the guarantee to seven years.

Under the public market contract for the purchase of IT equipment, the standard warranty is seven years.

3.7 Lifespan of materials, environmental aspects, equipment inventory exit

For ecological (responsible digital), economic and depreciation reasons, the IT equipment is replaced after the end of the guarantee period. Upon renewal, new items are released against return of old equipment. The equipment is renewed if it is no longer suitable for use and renewal is not automatic at the end of the warranty (7 years). The machines purchased on project are administered and maintained by the DNum which manages, as for the rest of the computer park, the life cycle of the latter.

3.8 Purchase of software

Any software order must go through the DNum, this makes it possible to check in particular whether a software is already present at the UTT, whether it complies with the security rules, or exists in the context of a contract to which the UTT has subscribed, and to ensure consistency with the licenses deployed. In the event of a problem or change in the conditions of use of software, the user must inform the DNum as soon as possible in order to regularize the situation.

3.9 Access

Each user is assigned an access code (a username and password) for the duration of his/her duties within the UTT or for the duration of his/her schooling when he/she is a student. The username and password are strictly personal and non-transferable. The password must be changed at least once a year and be sufficiently complex to ensure security. In particular, the password:

- must not be a common word or proper name in any language;
- must be at least eight characters long: combination of letters, numbers and special characters;
- must be different from that used on other sites, in particular commercial websites, in order to limit the risk of piracy.

Access takes account of the particular needs of each user and may change according to the situation of his/her situation.

Students and trainees can benefit from generic specific accounts for the duration of their training (practical work for example). These accounts are also password protected; they follow the same rules as any other user account.

In the event of a problem with his/her access account (identity theft, hacking, access difficulties), the user undertakes to notify DNum support as soon as possible. In the event of a risk resulting from the usurpation or hacking, the DNum may suspend the account and inform the user, if it has other means of contacting the user.

3.10 Connection to the UTT network

The DNum provides antivirus for maintained configurations. The use of this up-to-date antivirus software is mandatory when connecting this type of computer station by wire or Wi-Fi to the UTT network. The computer must be restarted at least once a week or in case of explicit request by the DNum, for safety reasons. It is strongly advised to turn off your computer instead of leaving it on standby as soon as your work session is over. For equipment not maintained by the DNum, it is the responsibility of the user to keep his/her operating system up to date and to ensure that his/her equipment does not present a risk to the UTT. The remote user must connect to the UTT, systematically through the Virtual Private Network (VPN) software to allow the update of the operating system and the antivirus system, when the computer is turned off.

The personal computer equipment is connected to the wifi network, InviteUTT, UTTpersonnels, UTTetudiants, or UTT personnels according to the statuses of the users. Academic visitors can be connected to the EDUROAM network (https://www.eduroam.fr/)

Professional IT equipment is connected to specific wifi networks, allowing access to the resources necessary for the activity to be managed and in a way that complies with the General Data Protection Regulation (GDPR).

Computer equipment purchased by external research organizations or companies may be connected to the UTT network with the same rights as those of the UTT, provided that the DNum becomes its administrator and that the inventory software is installed there, except in special cases authorized by the Chief Information Security Officer (RSSI) rssi@utt.fr (CISO) and the Defence Security Officer.

3.11 UTT e-mail

3.11.1 Professional character

Any exchange via e-mail is deemed to be professional to the exclusion of data explicitly designated by the user as part of his or her private life. It is up to the user to store his or her personal or private data in a space provided for this purpose and identified unambiguously: “private” or “personal”. The regular back-up of private data will be the responsibility of the user. The use of business messaging is not recommended for personal use.

3.11.2 Email management

The management of e-mails within the electronic mailbox (backup, deletion) is the responsibility of the user.

Since the storage capacity of the e-mail is limited for students and staff, once the quota is almost reached, an information e-mail is sent to him or her, he must then delete messages in order to free up space in his/her e-mail. Without any reaction on his/her part, his/her new emails will be returned to the sender, and will then be lost to the overquota user. The latter will have to present himself/herself to the DNum to reactivate the mailbox.

The availability of the user's mailbox is guaranteed except in the event of diagnosis and maintenance by the administrators or force majeure (imminent security problem).

3.11.3 Special duty to send e-mails

Users undertake to transmit messages and documents only to the persons for whom they are intended, and to target the contacts on their mailing lists. Similarly, the sending of attachments must be controlled and optimized by the user: compress them to lighten them before sending. Each email exchange generates an energy cost related to the transfer and backup of messages and attachments.

3.11.4 Principle of the right to integrity and confidentiality of files

The system administrator undertakes to respect the integrity and confidentiality of the files on the user's various accounts. However, within the limits of carrying out diagnosis or correction of problems, in specific security problems, on the latter or on the UTT information system, it will be possible for the administrator to access the files. The administrator will only open files named "private" or "personal" in case of particular risks or events (suspected espionage, leaked information) and in the presence of the user concerned (except in case of *force majeure*. If the university's antivirus software fails to decontaminate the file or if there is a proven risk that the information system will not function properly, the file will be destroyed.

3.12 Principle of the right to the availability of accounts and services on the UTT IS

The availability of files, folders and user work is guaranteed except in the event of diagnosis, maintenance by administrators on the network or *force majeure*. The availability of files is limited in time or due to specific conditions. The user acknowledges that all his/her files will no longer be accessible to him/her on the date of expiry of his/her rights on the UTT information system. These files may be deleted, archived, processed for anonymization, made available to the service for future use, after DPO notice.

The user deprived of his/her rights due to the violation of the provisions of these policies, automatically loses his/her access (for a limited time or indefinitely to the UTT information system and to all his/her files, folders, data.

3.13 Proper use

All users undertake to take care of the hardware and computer rooms made available to them and undertake to inform the DNum of any hardware or software problem and of theft or any damage committed, when they are detected.

Since the size of the disk and storage space available for each account is limited, the user must respect the size allocated to him/her and use the file compression and file size reduction tools available.

Reasonable use must be made of all shared IT resources in order to maintain optimal computing power, disk space and bandwidth on the UTT network. Each action on the information system consumes energy. Self-service workstations must be occupied for a period in accordance with individual and collective wishes. In addition, action authorized by law, that are part of the university's activities and that are likely to take a significant amount of IT resources will have to be carried out at times that least penalize users.

In general, in order to limit the energy impact of digital technology (responsible digital technology), it is recommended to:

- favor the dark mode of your display and the energy-saving mode of the computer;
- switch off computers rather than on standby;
- set up your video player with a low resolution;
- use an eco-responsible search engine;

- use an open-source browser using publicity blocking;
- clear/remove unnecessary and large files, including in your mailbox;
- give preference to textual formats.

3.14 Installation of software

It shall not be permitted:

- to use software that has been identified as dangerous for the security of the UTT and the list of which will be transmitted and updated by the DNum;
- to make a copy of software that is not royalty-free (NB: The creation of backup copies is a right of the administrator);
- to circumvent restrictions on the use of software;
- to develop or disseminate programs that are or may be related to viruses or malware.

It is necessary to consult the DNum before any software installation in order to guarantee a homogeneity of the application park, an optimal level of security and avoid a redundancy of functionalities. The DNum does not support applications of which it was not aware and the user assumes technical and legal responsibility for them. UTT has deployed widespread software protection not only on servers, but also on its own workstations. Therefore, it is prohibited to disable, alter the operation or uninstall this protection. The user must be aware of the energy and technical impact of downloading software, video streaming and music to the UTT bandwidth and of the risks it poses to the integrity of the information system since such software may be contaminated by Trojan horses, viruses and other ransomware.

3.15 Websites, E-portfolio and personal web pages

When creating websites or web pages that will eventually:

- hosted on UTT servers,
- or having a direct link with the university or its staff,

users undertake to declare the general theme of the site to the DNum and the Communication Service. This topic must be aligned with the UTT communication strategy.

Web pages that are public or intended for all users or a specific group, must comply with the design requirements the communication department, and are published under the sole responsibility of their authors.

By using the UTT E-portfolio system, users accept the terms of use as well as the rules concerning the protection of personal data. Users shall refrain from defamation, public insult or condemnable remarks. Any breach of this rule must be reported to the administrators who have the possibility to interrupt the broadcasting of the pages concerned and to suspend the user' account as a precautionary measure, without presuming possible prosecution before the disciplinary bodies of the UTT or before the courts.

Web pages intended to a single user or those shown by the mechanism of the secret URL are subject to the rules of private communication and are in particular protected by the secrecy of correspondence. Their recipients are therefore prohibited from showing them to third parties and undertake to guarantee their confidentiality. The UTT is not legally responsible for the content posted on the sites defined above, the content is posted under the responsibility of those who publish it.

4 Administration of the IS

Administrators are all persons who can intervene on one or more IT elements and resources, namely:

- individual workstations (desktop and laptop),
- computer servers,
- network,
- all material related to digitisation and printing,
- applications (server/client),
- databases,
- telephony.

They shall ensure the general proper functioning of the information system. Automatic security analysis scripts of the information system shall be used to detect any problems.

They have a duty to inform users and are bound to respect the confidentiality of the information they may hold or access. Administrators may have to interrupt completely or partially the use of the network, to temporarily stop the access to some applications for maintenance purposes. Users will then be informed in advance as far as possible.

The use of the various services generates trace files (computer logs) which are kept for the purpose of identifying users in case of infringement. Thus, in the event of an attempt to hack a private network via the UTT information system, the administrator must be able to provide the identity of the person through login logs, respecting the principle of confidentiality and the provisions listed above.

5 Consequences of non-compliance

The user who contravenes the rules previously defined is subject to the temporary or permanent suspension of his/her computer account and the computer devices made available to him/her as well as to multiple penalties, and/or civil and/or criminal proceedings, provided for by the laws and regulations in force.

6 Main legal texts of reference

Loi n° 2004-575 du 21 juin 2004 on confidence in the digital economy. - Art. 323-1 à 323-7 of the Criminal Code relating to computer fraud - Regulation (UE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data.

Loi 78-17 du 6 janvier 1978 amended law on information technology, files and freedoms.

Décret n°2005-1309 du 20 octobre 2005 implementing Law No 78-17 of 6 January 1978 on data processing, files and modified freedoms.

Art. 226-16 à 226-23 du Code pénal: infringements of personal rights resulting from both files and computer processing

Art. 226-24 du Code pénal establishing the criminal liability of legal persons for the same offences (art. 226-16 à 23)

Art. 335-2-1 et 335-3 du code de la propriété intellectuelle on the protection of software.

Art. 226-15 et 432-9 and the Criminal Code articles on secret correspondence (written, transmitted by telecommunication)

The intellectual property code

This list is not exhaustive.

The user and administrators acknowledge that they may incur disciplinary, civil and criminal penalties in the event of non-compliance with the policies.

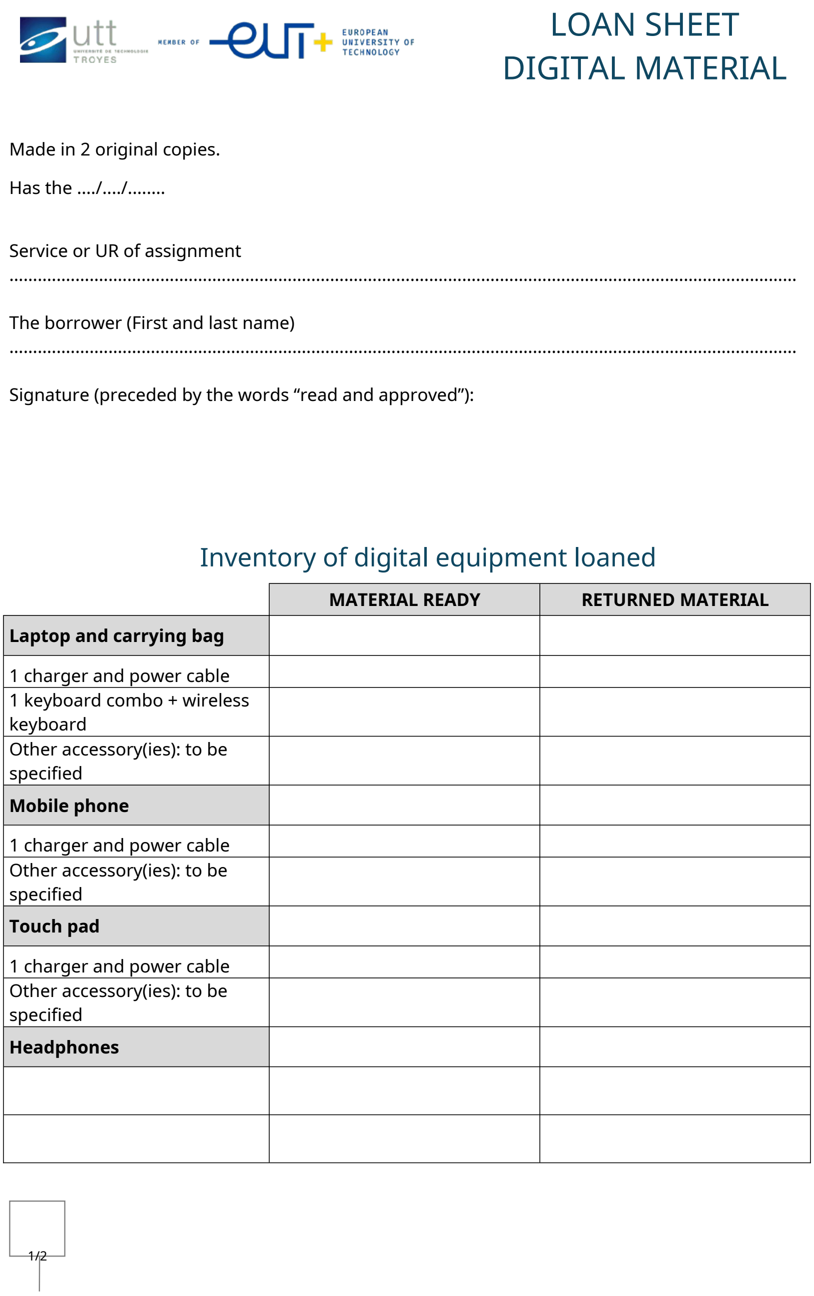
7 Final provisions

These policies and all related documents (right to disconnect) are available on the Digital Workplace (Environnement Numérique de Travail) (DW):

Documents UTT > Informatique et usage du numérique > Charte informatique (VPN is required for connection from outside UTT).

A IT equipment *loan* form

,



utt UNIVERSITÉ DE TECHNOLOGIE TROYES MEMBER OF EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

LOAN SHEET
DIGITAL MATERIAL

Made in 2 original copies.

Has the ..../..../........

Service or UR of assignment
....

The borrower (First and last name)
....

Signature (preceded by the words “read and approved”):

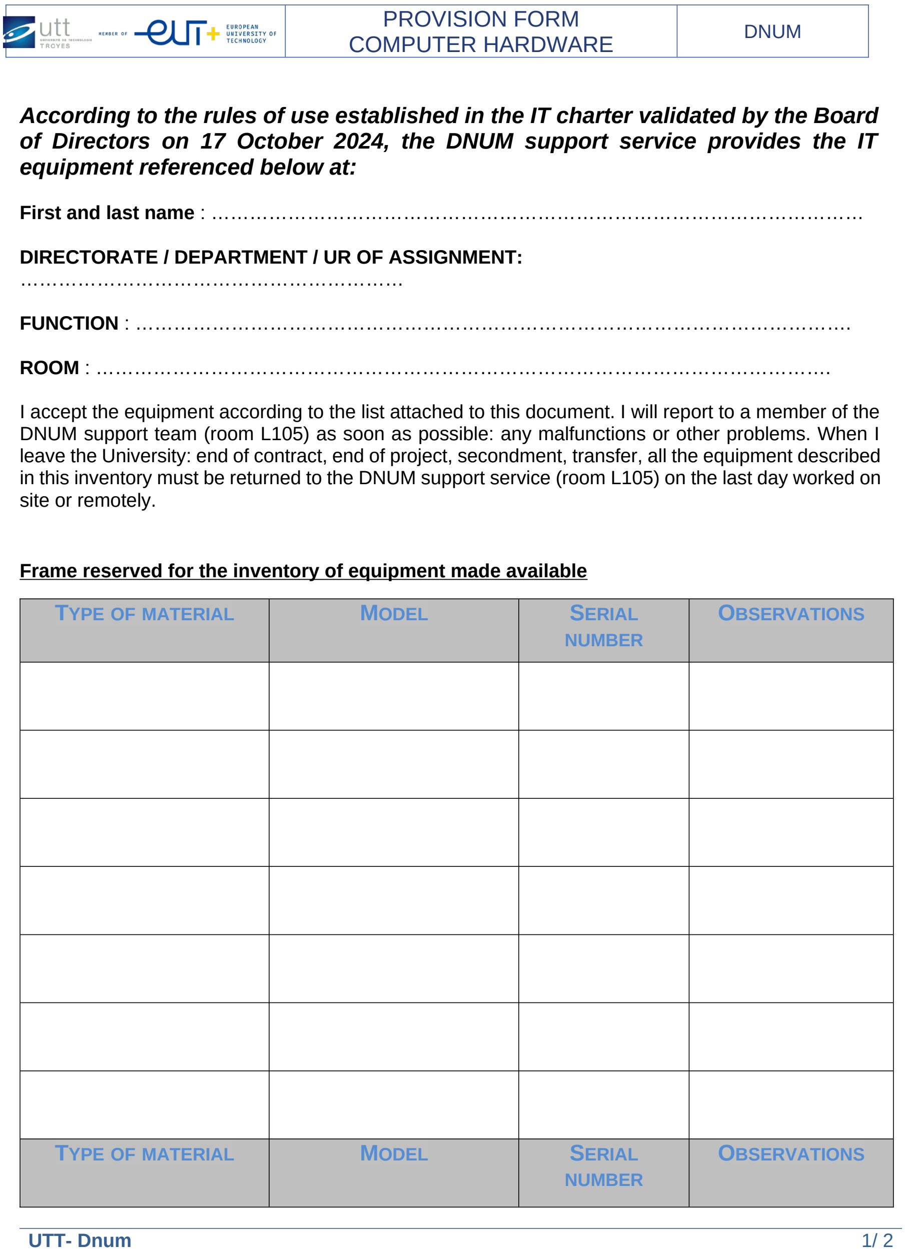
Inventory of digital equipment loaned

	MATERIAL READY	RETURNED MATERIAL
Laptop and carrying bag		
1 charger and power cable		
1 keyboard combo + wireless keyboard		
Other accessory(ies): to be specified		
Mobile phone		
1 charger and power cable		
Other accessory(ies): to be specified		
Touch pad		
1 charger and power cable		
Other accessory(ies): to be specified		
Headphones		

1/2

B IT equipment *availability* form

,



PROVISION FORM
COMPUTER HARDWARE

DNUM

According to the rules of use established in the IT charter validated by the Board of Directors on 17 October 2024, the DNUM support service provides the IT equipment referenced below at:

First and last name : ……………………………………………………………………………………………

DIRECTORATE / DEPARTMENT / UR OF ASSIGNMENT:
…………………………………………………….

FUNCTION : …………………………………………………………………………………………………….

ROOM : …………………………………………………………………………………………………….

I accept the equipment according to the list attached to this document. I will report to a member of the DNUM support team (room L105) as soon as possible: any malfunctions or other problems. When I leave the University: end of contract, end of project, secondment, transfer, all the equipment described in this inventory must be returned to the DNUM support service (room L105) on the last day worked on site or remotely.

Frame reserved for the inventory of equipment made available

TYPE OF MATERIAL	MODEL	SERIAL NUMBER	OBSERVATIONS
TYPE OF MATERIAL	MODEL	SERIAL NUMBER	OBSERVATIONS

UTT- Dnum 1/ 2